BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

10/661,650

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００３年　９月　５日

出願番号
Application Number: 特願２００３－３１４４６７

[ST. 10/C]: [ＪＰ２００３－３１４４６７]

出願人
Applicant(s): 株式会社リコー

２００３年１０月　７日

特許庁長官
Commissioner,
Japan Patent Office 今井康夫

出証番号　出証特２００３－３０８２７２９

【書類名】　特許願
【整理番号】　0304619
【提出日】　平成15年 9月 5日
【あて先】　特許庁長官　今井　康夫　殿
【国際特許分類】　G06F 12/00
【発明者】
　【住所又は居所】　東京都大田区中馬込１丁目３番６号　株式会社リコー内
　【氏名】　金井　洋一
【発明者】
　【住所又は居所】　東京都大田区中馬込１丁目３番６号　株式会社リコー内
　【氏名】　斉藤　敦久
【発明者】
　【住所又は居所】　東京都大田区中馬込１丁目３番６号　株式会社リコー内
　【氏名】　谷内田　益義
【特許出願人】
　【識別番号】　000006747
　【氏名又は名称】　株式会社リコー
【代理人】
　【識別番号】　100070150
　【弁理士】
　【氏名又は名称】　伊東　忠彦
【先の出願に基づく優先権主張】
　【出願番号】　特願2002-269102
　【出願日】　平成14年 9月13日
【先の出願に基づく優先権主張】
　【出願番号】　特願2002-299712
　【出願日】　平成14年10月11日
【手数料の表示】
　【予納台帳番号】　002989
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　特許請求の範囲　1
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
　【包括委任状番号】　9911477

【書類名】特許請求の範囲
【請求項１】
ドキュメントファイルに関連付けられている印刷要件を取得する手段と、
上記ドキュメントファイルを印刷する時に上記印刷要件を強制的に実行させる手段とを備えたことを特徴とするドキュメント印刷プログラム。
【請求項２】
暗号化された上記ドキュメントファイルの復号時に上記印刷要件を伴った印刷処理を実行することで上記印刷要件の強制を行う請求項１に記載のドキュメント印刷プログラム。
【請求項３】
暗号化された上記ドキュメントファイルの復号鍵を取得する手段と、
取得した復号鍵に基づいて上記ドキュメントファイルを復号する手段と、
上記ドキュメントファイルに関連付けられている上記印刷要件を取得する手段と、
取得した上記印刷要件を満たす印刷処理を実行させる手段とを備えた請求項２に記載のドキュメント印刷プログラム。
【請求項４】
復号された上記ドキュメントファイルから上記印刷要件を取得する請求項３に記載のドキュメント印刷プログラム。
【請求項５】
上記ドキュメントファイルを暗号化した暗号鍵に対応するパスワードを入力して復号鍵を生成する請求項４に記載のドキュメント印刷プログラム。
【請求項６】
内部で保持もしくは生成したパラメータを上記復号鍵の生成に利用する請求項５に記載のドキュメント印刷プログラム。
【請求項７】
上記ドキュメントファイルに関連付けられた上記印刷要件をネットワークを介してサーバから取得する請求項３に記載のドキュメント印刷プログラム。
【請求項８】
上記サーバに対してユーザの認証を行う手段と、
認証した上記ユーザの印刷要件を上記ドキュメントファイルに関連付けられて上記サーバに登録されたユーザ毎の印刷要件を含むＡＣＬから取得する手段とを備えた請求項７に記載のドキュメント印刷プログラム。
【請求項９】
上記ドキュメントファイルを暗号化した暗号鍵に相当するパラメータをネットワークを介してサーバから取得し、このパラメータから復号鍵を導出する請求項８に記載のドキュメント印刷プログラム。
【請求項１０】
内部で保持もしくは生成したパラメータを上記復号鍵の生成に利用する請求項９に記載のドキュメント印刷プログラム。
【請求項１１】
上記ドキュメントファイルに含まれるパラメータを上記復号鍵の生成に利用する請求項９または１０のいずれか一項に記載のドキュメント印刷プログラム。
【請求項１２】
ドキュメントファイルを暗号化する暗号鍵を取得する手段と、
指定された印刷要件を上記ドキュメントファイルに関連付ける手段と、
上記ドキュメントファイルを上記暗号鍵で暗号化する手段とを備えたことを特徴とするドキュメント保護プログラム。
【請求項１３】
上記ドキュメントファイルに上記印刷要件を付与してから暗号化することにより上記ドキュメントファイルと上記印刷要件とを関連付ける請求項１２に記載のドキュメント保護プログラム。

【請求項１４】
入力されたパスワードに基づいて暗号鍵を生成する請求項１３に記載のドキュメント保護プログラム。
【請求項１５】
内部で保持もしくは生成したパラメータを上記暗号鍵の生成に利用する請求項１４に記載のドキュメント保護プログラム。
【請求項１６】
上記ドキュメントファイルに関連付けられた上記印刷要件をネットワークを介してサーバに登録する請求項１２に記載のドキュメント保護プログラム。
【請求項１７】
上記印刷要件を上記ドキュメントファイルに関連付けたＡＣＬの一部として登録する請求項１６に記載のドキュメント保護プログラム。
【請求項１８】
暗号化に用いた暗号鍵を上記サーバに登録する請求項１７に記載のドキュメント保護プログラム。
【請求項１９】
暗号化に用いた暗号鍵の導出に用いたパラメータを上記サーバに登録する請求項１８に記載のドキュメント保護プログラム。
【請求項２０】
暗号化に用いた暗号鍵の導出に用いたパラメータを上記ドキュメントファイルの一部に付与する請求項１８または１９のいずれか一項に記載のドキュメント保護プログラム。
【請求項２１】
ドキュメントファイルを暗号化する暗号鍵を取得する手段と、指定された印刷要件を上記ドキュメントファイルに関連付ける手段と、上記ドキュメントファイルを上記暗号鍵で暗号化する手段とからなるドキュメント保護プログラムが実装された配布者端末と、
暗号化されたドキュメントファイルの復号鍵を取得する手段と、取得した上記復号鍵に基づいて上記ドキュメントファイルを復号する手段と、上記ドキュメントファイルに関連付けられている印刷要件を取得する手段と、取得した上記印刷要件を満たす印刷処理を実行させる手段とからなるドキュメント印刷プログラムが実装されたユーザ端末とを備えたことを特徴とするドキュメント保護システム。
【請求項２２】
ドキュメントファイルを暗号化する暗号鍵を取得する手段と、指定された印刷要件を上記ドキュメントファイルに関連付ける手段と、上記ドキュメントファイルを上記暗号鍵で暗号化する手段とからなるドキュメント保護プログラムが実装されたサーバと、
暗号化されたドキュメントファイルの復号鍵を取得する手段と、取得した上記復号鍵に基づいて上記ドキュメントファイルを復号する手段と、上記ドキュメントファイルに関連付けられている印刷要件を取得する手段と、取得した上記印刷要件を満たす印刷処理を実行させる手段とからなるドキュメント印刷プログラムが実装されたユーザ端末とを備えたことを特徴とするドキュメント保護システム。

【書類名】明細書
【発明の名称】ドキュメント印刷プログラム、ドキュメント保護プログラムおよびドキュメント保護システム
【技術分野】
【０００１】
本発明はドキュメント印刷プログラム、ドキュメント保護プログラムおよびドキュメント保護システムに関する。
【背景技術】
【０００２】
近年、文書や画像などの情報（以下、ドキュメントという）を取り扱うオフィスなどにおいては、ドキュメントを紙に印刷する代わりにドキュメントファイルとして情報記録媒体へ電子的に記録しておく手法が主流となっている。
【０００３】
ドキュメントを電子的に記録すれば、紙資源を用いることなくドキュメントを記録できるため、省資源化を図れるとともに、ドキュメントが印刷された紙を格納する必要がなくなり、省スペース化を実現できる。
【０００４】
また、ドキュメントを電子的に記録すれば、同一のドキュメントを多数人に対して同時に配布したり、遠隔地にいる者へネットワークを介してドキュメントを配布したりすることが可能となり、業務の効率化を図ることができる。
【０００５】
同一のドキュメントを多数人に対して同時に配布したり、遠隔地にいる者へネットワークを介してドキュメントを配布できるというドキュメントを電子的に記録する場合の長所は、ドキュメントが漏洩しやすくなるという問題の裏返しでもある。
【０００６】
オフィスなどにおいて取り扱われるドキュメントの中には、機密性を要するものも多数存在するため、ドキュメントの漏洩を防止するための対策を講じる必要がある。
【０００７】
ドキュメントの漏洩を防止することを目的とした従来技術としては、特許文献１に開示される「Method of encrypting information for remote access while maintaining access control」、特許文献２に開示される「Information security architecture for encrypting documents for remote access while maintaining access control」、および、特許文献３に開示される「文書管理システム」のように、ドキュメントファイルを開く際にユーザ認証を求めて、正当なユーザだけがドキュメントの内容を参照できるようにする手法や、開いたドキュメントファイルを印刷しようとする際にユーザに印刷する権限があるか否かをチェックして権限があるユーザにのみ印刷させるものがある。
【０００８】
また、特許文献４に開示される「電子的に伝送された情報の印刷制限方法および印刷制限付き文書」のように、支払いを済ませた場合にのみ印刷が許可されるようにドキュメンファイルをコントロールするような技術もある。
【特許文献１】米国特許第６３３９８２５号明細書
【特許文献２】米国特許第６２８９４５０号明細書
【特許文献３】特開２００１－１４２８７４号公報
【特許文献４】特開２００２－０２４０９７号公報
【発明の開示】
【発明が解決しようとする課題】
【０００９】
上記各特許文献に開示される発明においては、権限のない者がドキュメントを印刷できないように設定できるものの、印刷した物（プリントアウト）に対するセキュリティは何ら設定されていない。

【００１０】
よって、印刷する権限を有するユーザになりすまして一度ドキュメントを印刷してしまえば、その後は何の制約を受けることなくドキュメントのプリントアウトを複製して他者に配布できることになる。
【００１１】
さらに、ドキュメントを漏洩させようとする者が印刷する権限を有する正当なユーザである場合は、これを阻止することはできない。
【００１２】
このように、従来の技術では、ドキュメントファイルの使い勝手が良くないとともに、プリントアウトによるドキュメントの漏洩を防止するためのセキュリティが不十分であるという問題があった。
【００１３】
本発明はかかる問題に鑑みてなされたものであり、プリントアウトによるドキュメントの漏洩を防止したドキュメント印刷プログラム、ドキュメント保護プログラムおよびドキュメント保護システムを提供することを目的とする。
【課題を解決するための手段】
【００１４】
上記の目的を達成するため、本発明のドキュメント印刷プログラムは、ドキュメントファイルに関連付けられている印刷要件を取得する手段と、上記ドキュメントファイルを印刷する時に上記印刷要件を強制的に実行させる手段とを備えるようにしている。
【００１５】
これにより、印刷時におけるセキュリティ対策を強制することができる。
【００１６】
また、暗号化された上記ドキュメントファイルの復号時に上記印刷要件を伴った印刷処理を実行することで上記印刷要件の強制を行うようにすることができる。
【００１７】
これにより、暗号化技術を用いた堅牢なシステムが構築できる。
【００１８】
また、暗号化された上記ドキュメントファイルの復号鍵を取得する手段と、取得した復号鍵に基づいて上記ドキュメントファイルを復号する手段と、上記ドキュメントファイルに関連付けられている上記印刷要件を取得する手段と、取得した上記印刷要件を満たす印刷処理を実行させる手段とを備えるものとして構成できる。
【００１９】
また、本発明のドキュメント保護プログラムは、ドキュメントファイルを暗号化する暗号鍵を取得する手段と、指定された印刷要件を上記ドキュメントファイルに関連付ける手段と、上記ドキュメントファイルを上記暗号鍵で暗号化する手段とを備えるものとして構成できる。
【００２０】
また、本発明のドキュメント保護システムは、ドキュメントファイルを暗号化する暗号鍵を取得する手段と、指定された印刷要件を上記ドキュメントファイルに関連付ける手段と、上記ドキュメントファイルを上記暗号鍵で暗号化する手段とからなるドキュメント保護プログラムが実装された配布者端末と、暗号化されたドキュメントファイルの復号鍵を取得する手段と、取得した上記復号鍵に基づいて上記ドキュメントファイルを復号する手段と、上記ドキュメントファイルに関連付けられている印刷要件を取得する手段と、取得した上記印刷要件を満たす印刷処理を実行させる手段とからなるドキュメント印刷プログラムが実装されたユーザ端末とを備えるものとして構成できる。
【００２１】
また、ドキュメントファイルを暗号化する暗号鍵を取得する手段と、指定された印刷要件を上記ドキュメントファイルに関連付ける手段と、上記ドキュメントファイルを上記暗号鍵で暗号化する手段とからなるドキュメント保護プログラムが実装されたサーバと、暗

号化されたドキュメントファイルの復号鍵を取得する手段と、取得した上記復号鍵に基づいて上記ドキュメントファイルを復号する手段と、上記ドキュメントファイルに関連付けられている印刷要件を取得する手段と、取得した上記印刷要件を満たす印刷処理を実行させる手段とからなるドキュメント印刷プログラムが実装されたユーザ端末とを備えるものとしても構成できる。

【発明の効果】

【００２２】

本発明によれば、プリントアウトによるドキュメントの漏洩を防止したドキュメント印刷プログラム、ドキュメント保護プログラムおよびドキュメント保護システムを提供できる。

【発明を実施するための最良の形態】

【００２３】

〔第１の実施形態〕

本発明を好適に実施した第１の実施形態について説明する。

【００２４】

図１に、本実施形態にかかるドキュメント保護・印刷システムの構成を示す。

【００２５】

本実施形態にかかるドキュメント保護・印刷システムは、配布者端末１０１とユーザ端末１０２とプリンタ１０３とを有する。配布者端末１０１およびユーザ端末１０２は、表示装置（例えば、ＬＣＤ）、入力装置（例えば、キーボード）、外部記録装置（例えば、ＦＤＤ、ＨＤＤ）などを備えたコンピュータ端末を適用できる。なお、配布者端末１０１にはドキュメント保護プログラム１１１が、ユーザ端末１０２にはドキュメント印刷プログラム１２１がそれぞれ実装されている。

【００２６】

ドキュメント保護プログラム１１１は、ドキュメントファイルに配布者端末１０１の使用者（以下、配布者という）の入力操作に応じて印刷要件を設定するとともに、暗号化アルゴリズム（ＲＣ４、Ｔｒｉｐｌｅ　ＤＥＳ、ＩＤＥＡなど）を用いてドキュメントファイルを暗号化し、保護ドキュメントを生成する処理を行うプログラムである。図２はドキュメント保護プログラム１１１の構成例を示したものであり、属性付与部１１１ａと暗号化部１１１ｂと暗号鍵取得部１１１ｃとパラメータ取得部１１１ｄとを含んでいる。なお、パラメータ取得部１１１ｄは任意的要素である。各部の機能については後の動作において説明する。

【００２７】

図１に戻り、ドキュメント印刷プログラム１２１は、ユーザ端末１０２の使用者（以下、ユーザという）の入力操作に応じ、保護ドキュメントを復号するとともに設定されている印刷要件に応じた印刷処理をプリンタ１０３に実行させる処理を行うプログラムである。図３はドキュメント印刷プログラム１２１の構成例を示したものであり、復号部１２１ａと復号鍵取得部１２１ｂとパラメータ取得部１２１ｃと印刷要件取得部１２１ｄと印刷処理部１２１ｅとを含んでいる。なお、パラメータ取得部１２１ｃは任意的要素である。また、図４は図３における印刷処理部１２１ｅの構成例を示したものであり、要件処理部１２１ｆとドキュメント加工部１２１ｇとプリンタドライバ１２１ｈと警告表示部１２１ｉとログ記録部１２１ｊとを含んでいる。各部の機能については後の動作において説明する。

【００２８】

なお、配布者の入力操作に応じてドキュメント保護プログラム１１１がドキュメントファイルに設定する印刷要件の例としては、地紋印刷（Background Dot Pattern：以下、ＢＤＰという）、機密印刷（Private Access：以下、ＰＡＣという）、電子透かし（Digital Watermark：以下、ＤＷＭという）の付加、バーコード付加（Embedding Barcode：以下、ＥＢＣという）、機密ラベルスタンプ（Security Label Stamp：以下、ＳＬＳという）などが挙げられる。

【００２９】
本実施形態にかかるドキュメント保護・印刷システムの動作について説明する。まず、システム全体の動作について説明する。
【００３０】
図１において、配布者は、配布者端末１０１を操作してこれにドキュメントファイルを実装しておく。例えば、入力装置を用いて配布者がドキュメントファイルを作成してもよいし、外部記録装置を用いて情報記録媒体に記録されたドキュメントファイルを読み取らせても良い。
【００３１】
ドキュメントファイルにセキュリティを設定する場合、配布者は配布者端末１０１の入力装置を操作してドキュメントファイルをドキュメント保護プログラム１１１に受け渡す。ドキュメントファイルを取得したドキュメント保護プログラム１１１は、暗号化に用いられドキュメントファイルにアクセスするために必要となるパスワードと、印刷時に強制したいセキュリティ処理（すなわち、印刷要件）との設定を配布者に要求する。例えば、ドキュメント保護プログラム１１１は、配布者端末１０１の表示装置にメッセージを表示するなどして、パスワードと印刷要件の設定を要求する。図５はパスワードと印刷要件の設定を要求する画面の例を示したものであり、必要事項を入力したりチェックボックスから選択が行えるようになっている。なお、図５の画面では保護するドキュメントファイルを指定することもできるようになっている。
【００３２】
配布者が配布者端末１０１の入力装置を介してパスワードおよび印刷要件を入力すると、ドキュメント保護プログラム１１１はこれを取得する。なお、ドキュメント保護プログラム１１１はその後に生成する保護ドキュメントの保存場所を問い合わせるため、例えば図６に示すような画面を表示装置に表示する。
【００３３】
ドキュメント保護プログラム１１１は、取得したパスワードと印刷要件とを用いてドキュメントファイルから保護ドキュメントを生成する。
【００３４】
配布者は、ドキュメント保護プログラム１１１が生成した保護ドキュメントをユーザに受け渡すとともに、ドキュメントファイルにアクセスするために必要となるパスワードをユーザに通知する。
【００３５】
ユーザがドキュメントファイルを印刷しようとする場合には、ユーザ端末１０２に保護ドキュメントを実装する。例えば、情報記録媒体に記録された保護ドキュメントを外部記録装置を用いてユーザ端末に読み取らせても良いし、ユーザ端末１０２が配布者端末１０１と通信可能である場合には、通信網を介して配布者端末１０１から保護ドキュメントを取得するようにしてもよい。
【００３６】
ユーザが、ユーザ端末１０２の入力装置を介してドキュメント印刷プログラム１２１に対して印刷を指示すると、印刷を要求されたドキュメント印刷プログラム１２１は、ドキュメントファイルにアクセスするために必要となるパスワードの入力をユーザに要求する。例えば、ドキュメント印刷プログラム１２１は、ユーザ端末１０２の表示装置にメッセージを表示するなどして、パスワードの入力を要求する。図７はパスワードを要求する画面の例を示したものであり、印刷しようとしたドキュメントファイルが保護されている旨の説明文が伴われている。
【００３７】
ユーザが、配布者から通知されたパスワードを入力装置を介してユーザ端末１０２へ入力すると、ドキュメント印刷プログラム１２１は、入力されたパスワードを用いて保護ドキュメントをドキュメントファイルに復元し、設定されている印刷要件を満たすようにプリンタ１０３に印刷処理を実行させる。例えば、ドキュメントファイルに前述したＢＤＰ

が印刷要件として設定されている場合には、ドキュメントの内容とともに地紋画像を印刷する。

【００３８】

これにより、ドキュメントを印刷する際に、配布者が設定した印刷要件を強制することが可能となる。

【００３９】

なお、ユーザが印刷要件について意識していない場合があると共に、印刷要件によっては特定のプリンタでないと処理できないものもあるため、印刷の実行前にその旨の情報がユーザに提供されることが望ましい。図８はユーザ端末１０２の表示装置上に表示される確認画面の例を示したものであり、印刷要件と利用できるプリンタとが表示され、使用するプリンタを選択することができるようになっている。

【００４０】

次に、ドキュメント保護プログラム１１１の動作（保護ドキュメントを生成する処理）およびドキュメント印刷プログラム１２１の動作（保護ドキュメントを印刷する処理）についてさらに詳しく説明する。

【００４１】

図９に、ドキュメント保護プログラム１１１の動作を示す。

【００４２】

まず、ドキュメント保護プログラム１１１は、配布者が配布者端末１０１の入力装置を用いて設定した印刷要件をドキュメントファイルに添付する。

【００４３】

次に、配布者が配布者端末１０１の入力装置を用いて入力したパスワードを用いて、印刷要件が添付されたドキュメントファイルを暗号化して保護ドキュメントとする。

【００４４】

上記の動作を図２に基づいてさらに詳しく説明する。

【００４５】

まず、ドキュメント保護プログラム１１１の属性付与部１１１ａは、配布者から引き渡されたドキュメントファイル（doc）に、配布者によって設定された印刷要件（req）を属性として付与し、印刷要件の付与されたドキュメントファイル（doc+req）を暗号化部１１１ｂに渡す。

【００４６】

一方で暗号鍵取得部１１１ｃは、配布者によって入力されたパスワード（ku）および必要に応じて設けられたパラメータ取得部１１１ｄから得られるパラメータ（kp）に基づいて暗号鍵（k）を生成し、これを暗号化部１１１ｂに渡す。なお、パラメータ取得部１１１ｄのパラメータ（kp）はドキュメント保護プログラム１１１の内部に保持しておくか、要求があった場合に生成するようにする。ここで、暗号鍵（k）の生成アルゴリズムとしては、例えば、k=H｛ku,kp｝あるいはk=D｛ku,kp｝が使用できる。なお、H｛data1,data2,・・｝はdata1,data2,・・のハッシュ値を計算することを意味し、D｛data,key｝はkeyでdataを復号することを意味している。

【００４７】

そして、暗号化部１１１ｂは暗号鍵（k）に基づいて、印刷要件の付与されたドキュメントファイル（doc+req）を暗号化し、保護ドキュメント（enc）として出力する。式で示せばenc=E｛(doc+req),k｝となる。ここで、E｛data,key｝はkeyでdataを暗号化することを意味している。

【００４８】

図１０に、ドキュメント印刷プログラム１２１の動作を示す。

【００４９】

まず、ドキュメント印刷プログラム１２１は、ユーザがユーザ端末１０２の入力装置を用いて入力したパスワードを用いて保護ドキュメントを復号し、印刷要件が添付されたドキュメントファイルに復元する。次に、ドキュメント印刷プログラム１２１は、ドキュメ

ントファイルに設定されている印刷要件を満足するようにプリンタドライバを設定し（例えば、印刷要件として前述したＰＡＣが指定されていれば機密印刷モードに設定する）、ドキュメントを印刷する。なお、必要があれば、表示装置にメッセージを表示するなどして、印刷パラメータの設定をユーザに要求するようにしてもよい。

【００５０】

ドキュメントファイルに設定されている印刷要件を満足する印刷をプリンタ１０３では実行できない場合、換言すると、プリンタ１０３が設定された印刷要件を満たす機能を備えていない場合には、ドキュメント印刷プログラム１２１は、その旨を示すメッセージをユーザ端末１０２の表示装置に表示させるなどしてユーザに通知し、印刷は行わずに処理を終了する。

【００５１】

例えば、印刷要件としてＰＡＣが設定されている場合には、ドキュメント印刷プログラム１２１は、印刷を実行する前にＰＩＮ（個人識別番号：Personal Identification Number）の入力を要求する。この場合は、印刷実行後、プリンタ１０３のオペレーションパネルにおいて印刷実行前に入力したものと同一のＰＩＮが入力されるまでドキュメントのプリントアウトがプリンタ１０３から出力されない。このため、ドキュメントのプリントアウトがプリンタ１０３に不用意に放置されることがなくなり、プリントアウトによるドキュメントの漏洩を防止することが可能となる。

【００５２】

上記の動作を図３および図４に基づいてさらに詳しく説明する。

【００５３】

まず、図３において、ドキュメント印刷プログラム１２１の復号部１２１ａは、保護ドキュメント（enc）に対し、復号鍵取得部１２１ｂがパスワードおよび必要に応じて設けられたパラメータ取得部１２１ｃから得られるパラメータ（kp）から取得した復号鍵（k）を用いて復号を行う。なお、パラメータ取得部１２１ｃのパラメータ（kp）はドキュメント印刷プログラム１２１の内部に保持しておくか、要求があった場合に生成するようにする。ここで、復号鍵取得部１２１ｂにおける復号鍵（k）の生成アルゴリズムとしては、例えば暗号化の場合と同様に、k=H｛ku,kp｝あるいはk=D｛ku,kp｝が使用できる。なお、H｛data1,data2,・・｝はdata1,data2,・・のハッシュ値を計算することを意味し、D｛data,key｝はkeyでdataを復号することを意味している。

【００５４】

そして、復号部１２１ａは復号鍵（k）によって保護ドキュメント（enc）を復号し、印刷要件の付与されたドキュメントファイル（doc+req）を得て印刷処理部１２１ｅに渡す。なお、復号を式で示せば(doc+req)=D｛enc,k｝となる。ここで、D｛data,key｝はkeyでdataを復号することを意味している。一方、印刷要件取得部１２１ｄは復号されたドキュメントファイル（doc+req）から印刷要件（req）を取り出し、印刷処理部１２１ｅに渡す。

【００５５】

次いで、図４において、印刷処理部１２１ｅの要件処理部１２１ｆは、受け取った印刷要件の内容に応じて複数の処理を行う。すなわち、前述したＢＤＰ、ＥＢＣ、ＳＬＳのようにドキュメントファイルそのものを加工する必要がある処理についてはドキュメント加工部１２１ｇに加工情報を与えてドキュメントファイルの加工を行わせ、加工済みのドキュメントファイルをプリンタドライバ１２１ｈに渡し、印刷データをプリンタ１０３に与えて印刷を行う。また、ＰＡＣのようにプリンタドライバに特別な設定を行う必要がある処理についてはプリンタドライバ１２１ｈに印刷設定を行う。さらに、ユーザに対して警告メッセージを表示する必要がある場合には警告表示部１２１ｉに警告メッセージを渡し、表示装置に表示を行わせる。また、印刷のログを残す必要がある場合にはログ記録部１２１ｊにログ情報を渡し、リモートサーバ等にログデータを登録させる。

【００５６】

なお、以上の説明においては、図２および図３におけるパラメータ取得部１１１ｄおよびパラメータ取得部１２１ｃを任意的なものとしたが、これらを省略した場合、保護ドキ

ュメントをパスワードのみで復号できることを知っている者は、ドキュメント印刷プログラム１２１を介さずに、独自にパスワードを用いて保護ドキュメントを復号することも可能ではある。

【００５７】

仮にドキュメント印刷プログラム１２１を介することなく保護ドキュメントを復号した場合には、配布者が設定した印刷要件が強制されることなく、ドキュメントファイルを印刷できてしまう。

【００５８】

このため、パスワードのみでドキュメントファイルを暗号化するのではなく、例えば、図２におけるようなパラメータ取得部１１１ｄを設け、パスワードとドキュメント保護プログラム１１１の内部に埋め込まれている秘密鍵（パラメータ）とを合わせたもの（排他的論理和を取ったものなど）を用いてドキュメントファイルを暗号化するのが好ましい。

【００５９】

この場合は、ドキュメント印刷プログラム１２１にも図３に示すようなパラメータ取得部１２１ｃを設け、同一の秘密鍵（パラメータ）を埋め込んでおくことで、配布者が設定した印刷要件を印刷時に強制するドキュメント印刷プログラム１２１のみが、保護ドキュメントを復号して印刷することが可能となる。

【００６０】

さらに、プログラム内部に鍵データをそのまま格納したのでは攻撃者に察知される可能性があるため、鍵データをそのままプログラム内に保持するのではなく、必要になった際に計算して生成するようなアルゴリズムを組み込んでおくことが望ましい。その際、その生成アルゴリズムを特定されないよう、ソフトウェアの耐タンパー技術（解析されにくいようにプログラムを作成しておくことにより、攻撃者からの不正な解析からシステムを保護するための技術）を利用するといっそう安全性を高めることができる。

【００６１】

〔第２の実施形態〕

上記の第１の実施形態においては、ドキュメントファイルをパスワードを用いて保護するドキュメント保護・印刷システムについて説明したが、このシステムでは、パスワードを知っているか否かでドキュメントファイルを印刷できるか否かが決まることとなる。

【００６２】

しかし、実際には、「ユーザＡにはドキュメントファイルを印刷させてもよいが、ユーザＢには印刷させたくない。さらに、ユーザＣがドキュメントファイルを印刷しようとした場合には、プリントアウトに地紋を合成させるようにしたい。」といったように、ユーザ各人に応じて印刷要件を設定したい場合がある。本発明の第２の実施形態では、このような要求に対応できるドキュメント保護・印刷システムについて説明する。

【００６３】

図１１に、本実施形態にかかるドキュメント保護・印刷システムの構成を示す。

【００６４】

本実施形態にかかるドキュメント保護・印刷システムは、配布者端末２０１、ユーザ端末２０２、プリンタ２０３およびアクセスコントロールサーバ２０４を有する。

【００６５】

配布者端末２０１およびユーザ端末２０２は、第１の実施形態と同様に、表示装置（例えば、ＬＣＤ）、入力装置（例えば、キーボード）、外部記録装置（例えば、ＦＤＤ、ＨＤＤ）などを備えたコンピュータ端末を適用できる。なお、配布者端末２０１にはドキュメント保護プログラム２１１が、ユーザ端末２０２にはドキュメント印刷プログラム２２１がそれぞれ実装されている。

【００６６】

ドキュメント保護プログラム２１１は、ドキュメントファイルに配布者端末２０１の使用者（配布者）の入力操作に応じて処理要件を設定するとともに、暗号化アルゴリズム（ＲＣ４、Ｔｒｉｐｌｅ　ＤＥＳ、ＩＤＥＡなど）を用いてドキュメントファイルを暗号化

し、保護ドキュメントを生成する処理を行うプログラムである。図１２はドキュメント保護プログラム２１１の構成例を示したものであり、暗号化部２１１ａと暗号鍵取得部２１１ｂと属性付与部２１１ｃと属性登録部２１１ｄとを含んでいる。各部の機能については後の動作において説明する。

【００６７】

図１１に戻り、ドキュメント印刷プログラム２２１は、ユーザ端末２０２の使用者（ユーザ）の入力操作に応じ、保護ドキュメントを復号するとともに処理要件の一部として設定されている印刷要件に応じた印刷処理をプリンタ２０３に実行させる処理を行うプログラムである。図１３はドキュメント印刷プログラム２２１の構成例を示したものであり、復号部２２１ａと復号鍵取得部２２１ｂと印刷要件取得部２２１ｃと印刷処理部２２１ｄとを含んでいる。また、図１４は図１３における印刷処理部２２１ｄの構成例を示したものであり、要件処理部２２１ｅとドキュメント加工部２２１ｆとプリンタドライバ２２１ｇと警告表示部２２１ｈとログ記録部２２１ｉとを含んでいる。各部の機能については後の動作において説明する。

【００６８】

図１１に戻り、アクセスコントロールサーバ２０４は、ユーザがドキュメントにアクセス（例えば、印刷）しようとする場合に、ドキュメント印刷プログラム２２１からの要求に応じてアクセス制御リスト（Access Control List：ＡＣＬ）を参照し、ドキュメントにアクセスする権限があるか否か、処理要件がどのように設定されているかを取得するサーバである。

【００６９】

アクセスコントロールサーバ２０４には、ユーザ各人の認証用の情報（ユーザ名とパスワードとの組）が格納されたユーザデータベース２４１と、ユーザ各人ごとに設定された処理要件（印刷処理の要件を特に印刷要件という）を含むＡＣＬが登録されるＡＣＬデータベース２４２とが接続されている。

【００７０】

図１５はアクセスコントロールサーバ２０４の構成例を示したものであり、属性ＤＢ登録部２０４ａとユーザ認証部２０４ｂとアクセス権限確認部２０４ｃと印刷要件取得送付部２０４ｄとを含んでいる。各部の機能については後の動作において説明する。

【００７１】

なお、ＡＣＬの構造例を図１６に示す。ＡＣＬはユーザ名（User Name）、アクセスタイプ（Access Type）、許可情報（Permission）および処理要件（Requirement）をパラメータとして構成される。そして、このＡＣＬは、図１７に示すように、後述するドキュメントＩＤ（Document ID）および暗号鍵（Key）と関連付けられて一つのレコードとしてＡＣＬデータベース２４２に記録保持される。

【００７２】

本実施形態にかかるドキュメント保護・印刷システムの動作について説明する。最初にシステム全体の動作について説明する。

【００７３】

図１１において、配布者は、配布者端末２０１を操作してこれにドキュメントファイルを実装しておく。例えば、入力装置を用いて配布者がドキュメントファイルを作成してもよいし、外部記録装置を用いて情報記録媒体に記録されたドキュメントファイルを読み取らせても良い。

【００７４】

ドキュメントファイルにセキュリティを設定する場合、配布者は配布者端末２０１の入力装置を操作してドキュメントファイルをドキュメント保護プログラム２１１に受け渡す。ドキュメントファイルを取得したドキュメント保護プログラム２１１は、ＡＣＬの設定を配布者に要求する。例えば、ドキュメント保護プログラム２１１は、配布者端末２０１の表示装置にメッセージを表示するなどして、ＡＣＬの設定を要求する。図１８はＡＣＬの設定を要求する画面の例を示したものであり、ユーザ名、アクセス許可、印刷要件の設

定が行えるようになっている。すなわち、ＡＣＬのエントリとなるグループまたはユーザを追加し、そのグループまたはユーザに割り当てるアクセス権限を指定する。その際、必要に応じて印刷要件を指定することができ、印刷要件として設定可能なものの中から選択（チェック）を行い、更に補足情報が必要なものについては入力を行う。図ではウォーターマークの文字列として「ＣＯＮＦＩＤＥＮＴＩＡＬ」を指定している。そして、暗号化ボタンを押すことにより設定内容が取り込まれる。なお、この画面では保護するドキュメントファイルを指定することもできるようになっている。

【００７５】

配布者が配布者端末２０１の入力装置を介してＡＣＬを設定すると、ドキュメント保護プログラム２１１はこれを取得する。

【００７６】

ＡＣＬを取得したドキュメント保護プログラム２１１は、ドキュメントファイルごとに固有のドキュメントＩＤ（Document ID）と暗号化および復号に使用する暗号鍵（Key）とを生成し、ＡＣＬをこれらに関連付けてアクセスコントロールサーバ２０４へ送信し、ＡＣＬデータベース２４２への登録を要求する。

【００７７】

また、ドキュメント保護プログラム２１１は、暗号鍵を用いて暗号化したドキュメントファイルに対してドキュメントＩＤを付加して保護ドキュメントを生成する。

【００７８】

配布者は、ドキュメント保護プログラム２１１が生成した保護ドキュメントをユーザに受け渡す。

【００７９】

ユーザがドキュメントを印刷しようとする場合には、ユーザ端末２０２に保護ドキュメントを実装する。例えば、情報記録媒体に記録された保護ドキュメントを外部記録装置を用いてユーザ端末２０２に読み取らせても良いし、ユーザ端末２０２が配布者端末２０１と通信可能である場合には、通信網を介して配布者端末２０１から保護ドキュメントを取得するようにしてもよい。

【００８０】

ユーザが、ユーザ端末２０２の入力装置を介してドキュメント印刷プログラム２２１に対して印刷を指示すると、印刷を要求されたドキュメント印刷プログラム２２１は、ユーザを認証するために必要となるユーザ名とパスワードの入力をユーザに要求する。例えば、ドキュメント印刷プログラム２２１は、ユーザ端末２０２の表示装置にメッセージを表示するなどして、ユーザ名とパスワードの入力を要求する。図１９はユーザ名（ユーザＩＤ）とパスワードを要求する画面の例を示したものであり、キーボード等によって入力が行えるようになっている。

【００８１】

ドキュメント印刷プログラム２２１は、ユーザから入力されたユーザ名とパスワードとをアクセスコントロールサーバ２０４へ送信して、ユーザ認証を要求する。

【００８２】

アクセスコントロールサーバ２０４は、ドキュメント印刷プログラム２２１から受け渡されたユーザ名とパスワードとを用いてユーザ認証を行い、ユーザを特定する。

【００８３】

ユーザを特定すると、アクセスコントロールサーバ２０４は、ＡＣＬデータベース２４２を参照し、ドキュメントファイルを印刷する権限がユーザにあるか否かや、ユーザがドキュメントファイルを印刷する際には、どのような印刷要件が設定されているかを取得する。

【００８４】

ユーザにドキュメントファイルを印刷する権限がある場合、アクセスコントロールサーバ２０４は、その旨を示す認証情報とともに、保護ドキュメントを復号するための暗号鍵とユーザがドキュメントファイルを印刷する際の印刷要件とをユーザ端末２０２を介して

ドキュメント印刷プログラム２２１に通知する。

【００８５】

アクセスコントロールサーバ２０４から認証情報とともに、暗号鍵と印刷要件とを取得したドキュメント印刷プログラム２２１は、暗号鍵を用いて保護ドキュメントを復号してドキュメントファイルに復元する。

【００８６】

そしてドキュメント印刷プログラム２２１は、印刷要件を満たすようにプリンタ２０３に印刷処理を実行させる。例えば、ドキュメントファイルに前述したＢＤＰが印刷要件として設定されている場合には、ドキュメントの内容とともに地紋画像を印刷する。

【００８７】

これにより、ドキュメントファイルを印刷する際に、配布者がユーザ各人に対して設定した印刷要件を強制することが可能となる。

【００８８】

ここで、ドキュメントを保護する際のドキュメント保護プログラム２１１およびアクセスコントロールサーバ２０４の動作、および保護ドキュメントをドキュメントファイルに復元して印刷する際のドキュメント印刷プログラム２２１およびアクセスコントロールサーバ２０４の動作についてさらに詳しく説明する。

【００８９】

図２０に、ドキュメント保護プログラム２１１が保護ドキュメントを生成する際の動作を示す。ドキュメント保護プログラム２１１は、配布者端末２０１の入力装置における配布者の入力操作によってドキュメントファイルとＡＣＬとを取得すると、ドキュメントファイルを暗号化および復号するための暗号鍵を生成する。そして、ドキュメント保護プログラム２１１は、生成した暗号鍵を用いてドキュメントファイルを暗号化して、暗号化ドキュメントを生成する。

【００９０】

さらにドキュメント保護プログラム２１１は、ドキュメントファイルごとに固有のドキュメントＩＤを暗号化ドキュメントに添付して保護ドキュメントを生成する。

【００９１】

保護ドキュメントを生成した後、ドキュメント保護プログラム２１１は配布者端末２０１の通信機能を用いて、暗号鍵とＡＣＬとドキュメントＩＤとをアクセスコントロールサーバ２０４へ送信し、これらの登録をアクセスコントロールサーバ２０４に要求する。

【００９２】

暗号鍵とＡＣＬとドキュメントＩＤとをドキュメント保護プログラム２１１から受け渡されたアクセスコントロールサーバ２０４は、図１７に示したように、これらを関連付けて一つのレコードとしてＡＣＬデータベース２４２に記録保持する。

【００９３】

上記の動作を図１２および図１５に基づいてさらに詳しく説明する。

【００９４】

まず、図１２において、ドキュメント保護プログラム２１１の暗号化部２１１ａは、配布者から引き渡されたドキュメントファイルに対し、暗号鍵取得部２１１ｂが生成した暗号鍵を用いて暗号化を行い、この暗号化ドキュメントを属性付与部２１１ｃに渡す。

【００９５】

属性付与部２１１ｃはドキュメントＩＤを生成し、暗号化部２１１ａから渡された暗号化ドキュメントにドキュメントＩＤを付与して保護ドキュメントとして出力する。

【００９６】

また、属性登録部２１１ｄは配布者からＡＣＬを受け取るとともに、暗号鍵取得部２１１ｂから暗号鍵を、属性付与部２１１ｃからドキュメントＩＤをそれぞれ受け取り、アクセスコントロールサーバ２０４に対してこれらのドキュメントＩＤ、暗号鍵、ＡＣＬを渡して登録を要求する。

【００９７】

次いで、図１５において、アクセスコントロールサーバ２０４の属性ＤＢ登録部２０４ａは、渡されたドキュメントＩＤ、暗号鍵、ＡＣＬをＡＣＬデータベース２４２に登録する。

【００９８】

なお、上記の例においてはドキュメントＩＤの生成や暗号鍵の生成をドキュメント保護プログラム２１１が行う場合を示したが、これらの処理はアクセスコントロールサーバ２０４や不図示のサーバなどで行っても良い。

【００９９】

また、配布者端末２０１とアクセスコントロールサーバ２０４との間が専用回線ではなくネットワークを介して接続されており、暗号鍵などを送信する際に盗聴される懸念がある場合には、ＳＳＬ（Secure Socket Layer）を用いて通信を行えばよい。

【０１００】

ドキュメント保護プログラム２１１がアクセスコントロールサーバ２０４と通信する際のプロトコルは、どのようなものを用いてもよい。例えば、分散オブジェクト環境を導入し、Ｊａｖａ（Ｒ）ＲＭＩ（Remote Method Invocation）やＳＯＡＰ（Simple Object Access Protocol）をベースとして情報を送受信するようにしても良い。その場合、アクセスコントロールサーバ２０４は、例えば「register(String docId, byte[] key, byte[] acl)」のようなメソッドを実装するようにしてもよい。ＳＯＡＰであれば、ＨＴＴＰＳの上でＳＯＡＰプロトコルをやりとりし、ＲＭＩであればＳＳＬベースのSocketFactoryを用いてＲＭＩを実行するようにすれば、ネットワーク上でのセキュリティを確保できる。

【０１０１】

次に、ドキュメント印刷プログラム２２１が保護ドキュメントを印刷する際の動作について説明する。

【０１０２】

図２１に、保護ドキュメントを印刷する際のドキュメント印刷プログラム２２１およびアクセスコントロールサーバ２０４の動作の流れを示す。

【０１０３】

ドキュメント印刷プログラム２２１は、ユーザ端末２０２の入力装置におけるユーザの入力操作によって保護ドキュメントとユーザ名とパスワードとを取得すると、保護ドキュメントに添付されているドキュメントＩＤを取得する。

【０１０４】

そして、ユーザ名とパスワードとドキュメントＩＤとアクセスタイプ（ユーザが要求する処理を示す情報。ここでは、保護ドキュメントを印刷しようとするので、“print”となる。）とをアクセスコントロールサーバ２０４へ送信して、アクセス権限があるか否かのチェックを要求する。なお、図２２はアクセスコントロールサーバ２０４へのＳＯＡＰによる問い合わせの例を示す図であり、ユーザ名（userId）とドキュメントＩＤ（docId）とアクセスタイプ（accessType）とを渡してアクセスが許可されているかを問い合わせるＳＯＡＰメッセージ（isAllowed）を送付し、その結果（isAllowedResponse）を受け取っている例である。結果には、許可されているということ（allowedがtrue）と要件（requirements）とが含まれている。

【０１０５】

アクセスコントロールサーバ２０４は、ドキュメント印刷プログラム２２１からユーザ名とパスワードとドキュメントＩＤとアクセスタイプとを取得すると、ユーザデータベース２４１に登録されている情報を参照し、ユーザ認証を行う。

【０１０６】

換言すると、アクセスコントロールサーバ２０４は、ユーザデータベース２４１に登録されている情報を参照し、ドキュメント印刷プログラム２２１から取得した情報に含まれるユーザ名とパスワードとを組としたものが、ユーザデータベース２４１に組として登録されているか否かを判断する。

【０１０７】

ユーザ認証に失敗した場合（換言すると、ドキュメント印刷プログラム２２１から受け渡された情報に含まれるユーザ名とパスワードとを組としたものがユーザデータベース２４１に登録されていない場合）、アクセスコントロールサーバ２０４は、許可情報（ユーザが要求する処理を許可するか否かを示す情報）を「不許可」としてユーザ端末２０２へ送信し、ドキュメント印刷プログラム２２１へ受け渡す。なお、この場合は「エラー」とした許可情報をドキュメント印刷プログラム２２１へ受け渡すようにしてもよい。

【０１０８】

一方、ユーザ認証に成功した場合、アクセスコントロールサーバ２０４は、ＡＣＬデータベース２４２に格納されているレコードのうち、ドキュメント印刷プログラム２２１から取得した情報に含まれるドキュメントＩＤに関するレコードを読み出す。

【０１０９】

アクセスコントロールサーバ２０４は、読み出したレコードに含まれるＡＣＬを取得し、ドキュメント印刷プログラム２２１から取得したユーザ名およびアクセスタイプに基づいて、ＡＣＬから許可情報および印刷要件を取得する。

【０１１０】

換言すると、アクセスコントロールサーバ２０４は、ユーザ名とアクセスタイプとに基づいて、予めＡＣＬに設定されている許可情報と印刷要件とを取得する。

【０１１１】

ＡＣＬから取得した許可情報が「許可」である場合、アクセスコントロールサーバ２０４は、レコードに格納されている暗号鍵と印刷要件とを許可情報とともにユーザ端末２０２へ送信してドキュメント印刷プログラム２２１に受け渡す。

【０１１２】

一方、ＡＣＬから取得した許可情報が「不許可」である場合、アクセスコントロールサーバ２０４は、許可情報のみをユーザ端末２０２へ送信してドキュメント印刷プログラム２２１に受け渡す。

【０１１３】

アクセスコントロールサーバ２０４から許可情報を受け渡されたドキュメント印刷プログラム２２１は、取得した許可情報を参照し、「不許可」である場合には、ユーザ端末２０２の表示装置にメッセージを表示するなどして、要求された処理を実行できないことをユーザに通知する。

【０１１４】

一方、取得した許可情報が「許可」である場合には、許可情報と共に受け渡された暗号鍵を用いて、保護ドキュメントのうちの暗号化ドキュメントの部分を復号してドキュメントファイルに復元する。

【０１１５】

また、ドキュメント印刷プログラム２２１は、許可情報と共に取得した印刷要件を満足するようにプリンタドライバを設定し（例えば、ＰＡＣが指定されていれば機密印刷モードに設定する）、プリンタ２０３にドキュメントの印刷処理を実行させる。

【０１１６】

なお、必要があれば、ユーザ端末２０２の表示装置にメッセージを表示するなどして、印刷パラメータの設定をユーザに要求するようにしてもよい。

【０１１７】

アクセスコントロールサーバ２０４から取得した印刷要件を満足する印刷をプリンタ２０３では実行できない場合、換言すると、プリンタ２０３がＡＣＬに設定されていた印刷要件を満たす機能を備えていない場合には、その旨を示すメッセージを表示装置に表示させるなどしてユーザに通知し、印刷は行わずに処理を終了する。

【０１１８】

上記の動作を図１３～図１５に基づいてさらに詳しく説明する。

【０１１９】

まず、図１３において、ドキュメント印刷プログラム２２１の復号鍵取得部２２１ｂは

アクセスコントロールサーバ２０４に対してアクセス権の確認を行う。

【０１２０】

確認の問い合わせを受けたアクセスコントロールサーバ２０４は、図１５において、ユーザ認証部２０４ｂがユーザデータベース２４１を参照してユーザ認証を行い、認証結果をドキュメント印刷プログラム２２１に通知する。また、ユーザ認証に成功した場合、アクセス権限確認部２０４ｃがＡＣＬデータベース２４２を参照して許可情報および復号鍵を取得するとともに、印刷要件取得送付部２０４ｄが印刷要件を取得し、ドキュメント印刷プログラム２２１に通知する。なお、図１５ではいったん認証結果を返してから再び認証結果を渡すようにしているが、これを一度に実行してもよい。また、許可情報、復号鍵および印刷要件を別々に返すようにしているが、これらを一度に返すようにしてもよい。

【０１２１】

図１３において、復号鍵取得部２２１ｂはアクセス権の確認ができた場合にアクセスコントロールサーバ２０４から復号鍵を得て、これを復号部２２１ａに渡す。また、印刷要件取得部２２１ｃはアクセスコントロールサーバ２０４から印刷要件を取得し、印刷処理部２２１ｄに渡す。

【０１２２】

復号部２２１ａは復号鍵取得部２２１ｂから取得した復号鍵を用いて保護ドキュメントを復号し、ドキュメントファイルを得て印刷処理部２２１ｄに渡す。

【０１２３】

次いで、図１４において、印刷処理部２２１ｄの要件処理部２２１ｅは、受け取った印刷要件の内容に応じて複数の処理を行う。すなわち、前述したＢＤＰ、ＥＢＣ、ＳＬＳのようにドキュメントファイルそのものを加工する必要がある処理についてはドキュメント加工部２２１ｆに加工情報を与えてドキュメントファイルの加工を行わせ、加工済みのドキュメントファイルをプリンタドライバ２２１ｇに渡し、印刷データをプリンタ２０３に与えて印刷を行う。また、ＰＡＣのようにプリンタドライバに特別な設定を行う必要がある処理についてはプリンタドライバ２２１ｇに印刷設定を行う。さらに、ユーザに対して警告メッセージを表示する必要がある場合には警告表示部２２１ｈに警告メッセージを渡し、表示装置に表示を行わせる。また、印刷のログを残す必要がある場合にはログ記録部２２１ｉにログ情報を渡し、リモートサーバ等にログデータを登録させる。

【０１２４】

以上の動作によって、ユーザごとに異なるアクセス権や印刷要件を設定することが可能となる。また、上記のように、サーバ側でドキュメントファイルに対するアクセス権限を判断するシステム構成においては、ＡＣＬデータベース２４２に登録されているＡＣＬの内容を配布者端末２０１やアクセスコントロールサーバ２０４における入力操作によって変更できるようにしてもよく、この場合には、保護ドキュメントを配布した後で印刷要件を変更したりすることが可能となる。

【０１２５】

例えば、既に配布した保護ドキュメントに対するアクセス権限を新たなユーザに設定したり、特定のユーザに対して印刷要件を追加することなどが可能となる。

【０１２６】

なお、本実施形態にかかるドキュメント保護・印刷システムが上記のような手法でドキュメントファイルを保護していることを知っている者は、ドキュメント印刷プログラム２２１に成りすますプログラムをコンピュータ端末に実行させて暗号鍵を不正に入手し、保護ドキュメントを復号することも可能ではある。この場合は、ＡＣＬとして設定されている印刷要件を強制されることなく、保護ドキュメントを印刷できてしまうこととなる。

【０１２７】

このため、単に暗号鍵のみを用いてドキュメントファイルを暗号化するのではなく、ドキュメント保護プログラム２１１の内部に埋め込まれた秘密鍵と暗号鍵とを合わせたもの（排他的論理和を取ったもの）でドキュメントファイルを暗号化することが好ましい。この場合は、ドキュメント印刷プログラム２２１にも同一の秘密鍵を埋め込んでおくこと

で、配布者が設定した印刷要件を印刷時に強制するドキュメント印刷プログラム２２１のみが、保護ドキュメントを復号して印刷することが可能となる。

【０１２８】

図２３および図２４は上述したような内部に秘密鍵を埋め込んでおくタイプの構成例を示したものであり、図２３はドキュメント保護プログラム２１１の構成例を示し、図２４はドキュメント印刷プログラム２２１の構成例のうち復号に関係する部分のみを示している。なお、この例は、単に内部に秘密鍵を埋め込んでおくだけではなく、乱数を導入して不正アクセスに対しより強化している。

【０１２９】

図２３において、ドキュメント保護プログラム２１１は暗号化部２１１ａと暗号鍵取得部２１１ｂと属性付与部２１１ｃと属性登録部２１１ｄとパラメータ取得部２１１ｅとを含んでいる。

【０１３０】

動作にあっては、パラメータ取得部２１１ｅはパラメータ（kp）を生成し、暗号鍵取得部２１１ｂに渡す。なお、パラメータ（kp）はドキュメント保護プログラム２１１の内部に保持しておくか、要求があった場合に生成するようにする。

【０１３１】

暗号鍵取得部２１１ｂはパラメータ取得部２１１ｅからパラメータ（kp）を受け取った上で、二つの乱数（kd）（ks）を生成し、暗号鍵（k）を式k=H{ks,kp,kd}あるいはk=D{kd,D{ks,kp}}で計算して生成し、暗号鍵（k）を暗号化部２１１ａに、乱数（kd）を属性付与部２１１ｃに、乱数（ks）を属性登録部２１１ｄにそれぞれ渡す。なお、H{data1,data2,・・}はdata1,data2,・・のハッシュ値を計算することを意味し、D{data,key}はkeyでdataを復号することを意味している。

【０１３２】

暗号化部２１１ａは配布者から引き渡されたドキュメントファイル（doc）に対し、暗号鍵取得部２１１ｂから取得した暗号鍵（k）を用いて暗号化を行い、暗号化されたドキュメント（enc）を属性付与部２１１ｃに渡す。式で示せばenc=E{doc,k}となる。なお、E{data,key}はkeyでdataを暗号化することを意味している。

【０１３３】

次いで、属性付与部２１１ｃはドキュメントＩＤ（id）を生成し、暗号化されたドキュメント（enc）にそのドキュメントＩＤ（id）と暗号鍵取得部２１１ｂから渡された乱数（kd）を付与して保護ドキュメント（enc+id+kd）を出力する。また、属性付与部２１１ｃは生成したドキュメントＩＤ（id）を属性登録部２１１ｄに渡す。

【０１３４】

属性登録部２１１ｄは、属性付与部２１１ｃから渡されたドキュメントＩＤ（id）と暗号鍵取得部２１１ｂから渡された乱数（ks）と配布者から取得したＡＣＬ（attr）とをアクセスコントロールサーバ２０４に通知し、登録を要求することになる。

【０１３５】

復号にあっては、図２４において、復号鍵取得部２２１ｂは保護ドキュメントから乱数（kd）を取得するとともに、パラメータ取得部２２１ｊからドキュメント印刷プログラム２２１の内部に保持してある、あるいは要求に応じて生成したパラメータ（kp）を取得し、さらにアクセスコントロールサーバ２０４から乱数（ks）を取得し、暗号化の場合と同様に式k=H{ks,kp,kd}あるいはk=D{kd,D{ks,kp}}で計算して復号鍵（暗号鍵）（k）を得る。

【０１３６】

そして、復号部２２１ａは暗号化されたドキュメント（enc）を復号鍵（k）で復号し、ドキュメントファイル（doc）を得る。

【０１３７】

図２３および図２４は、アクセスコントロールサーバ２０４に登録される乱数（ks）と保護ドキュメント内の乱数（kd）とドキュメント保護プログラム２１１もしくはドキュメ

ント印刷プログラム２２１内から取得されるパラメータ（kp）とに基づいて暗号鍵（復号鍵）（k）を生成する方式であるが、こうすることでアクセスコントロールサーバ２０４が悪意のあるユーザによって不正アクセスされて乱数（ks）が知られてしまった場合であっても、乱数（kd）やパラメータ（kp）が知られなければ保護ドキュメントを復号できないことになる。なお、アクセスコントロールサーバ２０４が不正アクセスされないように十分にガードされている環境にあっては、乱数（ks）をそのまま暗号鍵（復号鍵）（k）として使用してもよい。

【０１３８】

一方、これまで説明してきた第２の実施形態では、印刷要件をアクセスコントロールサーバ２０４にのみ格納するものとしてきたが、そのような形式に限定されず、保護ドキュメントに含めるようにしてもよい。例えば、ユーザによらずドキュメントファイルに対して必ず指定するような印刷要件については保護ドキュメントの中に含めるようにしてもよい。

【０１３９】

図２５は、印刷要件を保護ドキュメントに含める第一印刷要件と、アクセスコントロールサーバ２０４に格納される第二印刷要件とに分けた場合のドキュメント印刷プログラム２２１の構成例を示したものであり、印刷要件取得部２２１ｃにおいてアクセスコントロールサーバ２０４から第二印刷要件を取得するとともに、復号部２２１ａにおいて保護ドキュメントから第一印刷要件を取得し、第一印刷要件および第二印刷要件に基づいて印刷処理部２２１ｄで印刷処理を行うようにしている。その他は図１３に示したドキュメント印刷プログラム２２１と同様である。

【０１４０】

また、本実施形態においては、ドキュメント印刷プログラム２２１は、ドキュメントファイルの印刷に関する処理のみを行っているが、ドキュメント印刷プログラム２２１は、ドキュメントファイルの内容をユーザに提示したり、ドキュメントファイルを編集する機能を備えていても良い。例えば、Adobe Acrobat（Ｒ）のPlug-inとしてポータブルドキュメントファイル（Portable Document Format：ＰＤＦ File）の表示、編集および印刷の機能を実現することが可能である。

【０１４１】

図２６に、上記各実施形態において適用されるプリンタが備えるセキュリティ機能の一部を示す。これらについて第２の実施形態におけるシステム構成を例として具体的に説明する。

【０１４２】

まず、印刷要件としてＰＡＣが設定されている場合のドキュメント印刷プログラム２２１の動作について説明する。ＰＡＣが設定されている場合のドキュメント印刷プログラム２２１の動作を図２７に示す。

【０１４３】

（１）ドキュメント印刷プログラム２２１はＰＡＣが設定されているドキュメントファイルを印刷する際には、図２８に示すように、プリントダイアログを表示させた後に個人識別番号（Personal Identification Number：ＰＩＮ）を入力するダイアログをユーザ端末２０２の表示装置に表示させ、ユーザにＰＩＮの入力を要求する。

【０１４４】

（２）ユーザ端末２０２の入力装置を用いてユーザがＰＩＮを入力すると、ドキュメント印刷プログラム２２１は、これをプリンタドライバに設定し、印刷を指示する。

【０１４５】

プリンタドライバは、ドキュメントからPostscriptなどのＰＤＬ（Page Description Language）で記述された印刷データ（ＰＤＬデータ）を生成し、印刷部数や出力トレイなどの印刷ジョブ情報を記述したＰＪＬ（Print Job Language）データをＰＤＬデータの先頭に付加する。プリンタドライバはさらにＰＪＬデータの一部としてＰＩＮを付加し、そのＰＪＬデータ付きＰＤＬデータをプリンタ２０３に送る。

【０１４６】
プリンタ２０３は、ＰＪＬデータ付きＰＤＬデータを受け取るとＰＪＬデータの内容を参照し、機密印刷用のＰＩＮが含まれている場合は印刷出力せずにプリンタ２０３内部の記憶装置（ＨＤＤなど）にＰＪＬデータ付きＰＤＬデータを保存する。ユーザがＰＩＮをプリンタ２０３のオペレーションパネルを介して入力すると、プリンタ２０３は入力されたＰＩＮをＰＪＬデータに含まれるＰＩＮと照合し、一致すればＰＪＬデータに含まれていた印刷ジョブ条件（部数、トレイなど）を適用しながらＰＤＬデータに従って印刷出力する。

【０１４７】
（３）プリンタドライバにＰＩＮが設定できない、すなわち、プリンタ２０３が機密印刷をサポートしていない場合には、機密印刷をサポートしている別のプリンタを選択するようにユーザに通知し、ドキュメントを印刷せずに処理を終了する。

【０１４８】
このようにすることで、印刷実行後、プリンタ２０３のオペレーションパネルにおいて印刷実行前に入力したものと同一のＰＩＮが入力されるまでドキュメントのプリントアウトがプリンタ２０３から出力されなくなる。このため、ドキュメントのプリントアウトがプリンタ２０３に不用意に放置されることがなくなり、プリントアウトによるドキュメントの漏洩を防止することが可能となる。さらに、ネットワーク上を流れるプリントデータを盗聴されないようにプリンタ２０３とのやりとりをＳＳＬで保護してもよい。

【０１４９】
また、ドキュメント印刷プログラム２２１をWindows（Ｒ）Domainのユーザ管理と連動させて、ユーザに対してＰＩＮの入力を要求しないようにしてもよい。例えば、ＰＩＮをユーザに入力させるのではなく、Windows（Ｒ）Domainから現在ログオン中のユーザＩＤを取得し、プリントデータとともにユーザＩＤをプリンタ２０３へ送付するようにする。プリンタ２０３は、オペレーションパネルでユーザからのパスワード入力を受け、そのユーザＩＤとパスワードとでWindows（Ｒ）Domainのユーザ認証機構を用いてユーザ認証を行い、成功すればプリントアウトするようにしても良い。Windows（Ｒ）Domainに限定されず、予め導入されているユーザ管理と連動させることで、ユーザにとって面倒なＰＩＮ入力の手間を削減できる。

【０１５０】
次に、印刷要件としてＥＢＣが設定されている場合のドキュメント印刷プログラム２２１の動作について説明する。

【０１５１】
（１）ドキュメント印刷プログラム２２１は、ＥＢＣが設定されているドキュメントを印刷する際にドキュメントＩＤを示すバーコード画像データ（又は、二次元コード）のデータを生成する。

【０１５２】
（２）ドキュメント印刷プログラム２２１は、生成したバーコード画像データをスタンプ画像としてプリンタドライバにセットし、プリンタ２０３に印刷を指示する。

【０１５３】
（３）プリンタドライバにＥＢＣが設定できない、すなわち、プリンタ２０３がスタンプ機能をサポートしていない場合は、スタンプ機能をサポートしている他のプリンタを選択するようにユーザに通知し、印刷を行わずに処理を終了する。

【０１５４】
このようにすることで、ドキュメントのプリントアウトの各ページにはバーコードが印刷されるため、このバーコードを識別できる複写機、ファックス、スキャナのみがバーコードをデコードすることでドキュメントＩＤを取得し、そのドキュメントＩＤを基にアクセスコントロールサーバ２０４でハードコピー、画像読み取り、ファックス送信などが許可されているか否かを判断することが可能となる。これにより、紙文書まで一貫したセキュリティ確保が可能となる。

【０１５５】
次に、印刷要件としてＢＤＰが設定されている場合のドキュメント印刷プログラム２２１の動作について説明する。
【０１５６】
（１）ドキュメント印刷プログラム２２１は、ＢＤＰが設定されているドキュメントを印刷する際に、印刷を要求しているユーザ名と印刷日時とを文字列として取得する（例えば、Ichiro,2002/08/04 23:47:10）。
【０１５７】
（２）ドキュメント印刷プログラム２２１は、ドキュメントのプリントアウトを複写機で複写した際に、生成した文字列が浮き上がるように地紋画像を生成する。
【０１５８】
（３）ドキュメント印刷プログラム２２１は、生成した地紋画像をスタンプとしてプリンタドライバにセットし、プリンタ２０３にドキュメントの印刷を指示する。
【０１５９】
（４）プリンタドライバにＢＤＰが設定できない場合、すなわちプリンタ２０３が地紋印刷をサポートしていない場合には、地紋印刷をサポートしている別のプリンタを選択するようにユーザに通知し、印刷を行わずに処理を終了する。
【０１６０】
このようにすることで、ドキュメントのプリントアウトの各ページには、印刷処理を実行したユーザ名と日時とが浮き出る地紋画像として印刷され、プリントアウトを複写機やスキャナ、ファックスで処理すると文字列が浮き出ることとなる。これ、ＥＢＣをサポートしていない複写機を使用する場合などに有効であり、ドキュメントのプリントアウトを複写することによる情報漏洩に対して抑止力を有する。
【０１６１】
次に、印刷要件としてＳＬＳが設定されている場合のドキュメント印刷プログラム２２１の動作について説明する。
【０１６２】
（１）ドキュメント印刷プログラム２２１は、ＳＬＳが設定されているドキュメントファイルを印刷する際に、予め用意された画像のうち、そのドキュメントの機密レベルに応じたもの（Top Secretならば「極秘」のマークなど）を選択する。
【０１６３】
（２）選択した画像のデータを、スタンプとしてプリンタドライバにセットし、プリンタ２０３に印刷を指示する。
【０１６４】
（３）プリンタドライバにＳＬＳをセットできない場合、すなわち、プリンタ２０３がＳＬＳをサポートしていない場合には、ラベルスタンプをサポートしている別のプリンタを選択するようにユーザに通知し、印刷を行わずに処理を終了する。
【０１６５】
このようにすることで、ドキュメントファイルのプリントアウトには、自動的に「極秘」や「マル秘」がスタンプとして印刷されるため、ドキュメントが機密文書であることが明らかとなる。すなわち、プリントアウトを所持する者に管理上の注意を喚起することができる。
【０１６６】
上記の各例は、あくまでも印刷要件の例であり、改ざん防止用の電子透かしを印刷するようにしたり、保護されているドキュメントは特殊な用紙に印刷する（印刷に使用する用紙トレイを特殊用紙のトレイに限定する）ようにしてもよい。
【０１６７】
さらに付言すると、印刷要件には、機能を制限・禁止するものと、機能を強制的に使用させるもの、加えて通常の印刷条件指定などを含めることができる。機能を制限・禁止する例としては、機密文書原本と区別をするために特別なユーザのみカラーでの印刷を許可

して、他のユーザはグレースケールでの印刷のみを許可するように制限するための印刷要件などである。機能を強制的に使用させる例としては、機密印刷モードを強制的に使用するような印刷要件や、ログを強制的に記録するような印刷要件、印刷紙面に印刷したユーザの名前を強制的に印字するような印刷要件、ウォーターマークを強制的に印刷する印刷要件、地紋を強制的に印刷する印刷要件などである。通常の印刷条件を指定する例としては、用紙設定としてＡ４を指定する印刷要件，再生紙トレイを使用する印刷要件，両面印刷を指定する印刷要件などである。

【０１６８】

また、これまで印刷要件の表現形式としてＲＡＤ、ＰＡＣといったキーワードを用いて説明してきたが、そのようなキーワードでなくとも、例えば、プリンタドライバに設定する設定ファイルのデータそのものや、プリントデータに挿入するページ記述言語で表現したデータ、画面に表示する文字列そのもの、処理すべき要件の内容をスクリプト言語で記述したデータのようなものを用いて印刷要件を表現して規定するようにしても良い。すなわち、印刷要件の表現をキーワードのようなものに限定するものではない。

【０１６９】

このように、プリンタ２０３がサポートする様々なセキュリティ機能を利用してセキュリティポリシーに沿った印刷要件を設定することによって、プリンタ２０３のセキュリティ機能を無駄なく活用して、プリントアウトに至るまで一貫したセキュリティの確保が可能となる。これは他の実施形態のシステム構成においても同様である。

【０１７０】

一方、これまでの説明において、保護対象はドキュメント全体であるように記述してきたが、ドキュメントの中に保護対象となる部分（セグメントと呼ぶ）と、保護対象としない部分が混在していても良い。例えば、図２９に示すように、保護セグメントが複数保護ドキュメント内に存在していても良い。この場合、保護セグメントごとに異なるセグメントＩＤをつけ、これまでの説明におけるドキュメントＩＤをセグメントＩＤと読みかえれば、同じ原理で保護セグメントごとに印刷を含むアクセスの制御が可能になる。実際には、保護セグメントの先頭と末尾には、そこから保護セグメントが開始することを示しそこで保護セグメントが終了することを示すマーカのようなものをつける必要がある。そういったマーカの入れ方については、ＭＩＭＥのマルチパートセパレータなどの従来技術を用いることができる。

【０１７１】

また、これまではドキュメント保護プログラムが配布者端末に配置されるような実施例に基づいて説明してきたが、ドキュメント保護プログラム本体はリモートサーバ上に配置するようにしても良い。例えば図１１の配布者端末２０１、ドキュメント保護プログラム２１１およびアクセスコントロールサーバ２０４の関係は、図３０に示すように変形することができる。このように配置することにより、ドキュメント保護プログラムがインストールされていない端末からでもリモートサーバにドキュメントと必要なパラメータを送付して保護ドキュメントを取得することができる。

【０１７２】

なお、上述した各実施形態は、本発明の好適な実施の例であり、本発明はこれらに限定されることはない。

【０１７３】

例えば、上記各実施形態においては、配布者端末とユーザ端末とが別個の装置である場合を例に説明を行ったが、これらは同一の装置を共用するような構成であっても構わない。

【０１７４】

また、上記各実施形態では、ドキュメント印刷プログラムが実装されたユーザ端末を、ユーザが直接操作する場合を例に説明を行ったが、これに限定されるものではない。例えば、ドキュメント印刷プログラムがサーバに実装されており、ユーザがユーザ端末を操作しネットワークを介してドキュメント印刷プログラムを実行させる構成であってもよい。

【０１７５】
また、ユーザ認証の方法は、ユーザ名とパスワードとを用いる方法に限定されることはなく、スマートカードを用いたＰＫＩベースの認証方法を適用してもよい。
【０１７６】
このように、本発明は様々な変形が可能である。
【０１７７】
さらに、上記の説明では「プリンタ」という用語が使われているが、これは狭義のプリンタ専用機に限らず、コピー、ファクシミリ、これらの複合・融合された機器等、すなわち印刷機能を有するすべての機器を意味するものである。
【図面の簡単な説明】
【０１７８】
【図１】本発明を好適に実施した第１の実施形態にかかるドキュメント保護・印刷システムの構成を示す図である。
【図２】ドキュメント保護プログラムの構成例を示す図である。
【図３】ドキュメント印刷プログラムの構成例を示す図である。
【図４】印刷処理部の構成例を示す図である。
【図５】パスワードと印刷要件の設定を要求する画面の例を示す図である。
【図６】保護ドキュメントの保存場所を問い合わせる画面の例を示す図である。
【図７】パスワードを要求する画面の例を示す図である。
【図８】ユーザ端末の表示装置上に表示される確認画面の例を示す図である。
【図９】第１の実施形態にかかるドキュメント保護プログラムの動作を示す図である。
【図１０】第１の実施形態にかかるドキュメント印刷プログラムの動作を示す図である。
【図１１】本発明を好適に実施した第２の実施形態にかかるドキュメント保護・印刷システムの構成を示す図である。
【図１２】ドキュメント保護プログラムの構成例を示す図である。
【図１３】ドキュメント印刷プログラムの構成例を示す図である。
【図１４】印刷処理部の構成例を示す図である。
【図１５】アクセスコントロールサーバの構成例を示す図である。
【図１６】ＡＣＬの構成例を示す図である。
【図１７】ＡＣＬデータベースに記録される情報の構造例を示す図である。
【図１８】ＡＣＬの設定を要求する画面の例を示す図である。
【図１９】ユーザ名（ユーザＩＤ）とパスワードを要求する画面の例を示す図である。
【図２０】第２の実施形態にかかるドキュメント保護プログラムの動作を示す図である。
【図２１】第２の実施形態にかかるドキュメント印刷プログラムおよびアクセスコントロールサーバの動作の流れを示す図である。
【図２２】アクセスコントロールサーバへのＳＯＡＰによる問い合わせの例を示す図である。
【図２３】ドキュメント保護プログラムの構成例を示す図である。
【図２４】復号の様子を示す図である。
【図２５】ドキュメント印刷プログラムの構成例を示す図である。
【図２６】プリンタが備えるセキュリティ機能の例を示す図である。
【図２７】ＰＡＣが設定されたドキュメントを印刷する際の処理を示す図である。
【図２８】ＰＩＮ入力のダイアログを示す図である。
【図２９】ドキュメントを複数のセグメントに分けて保護する場合の処理を示す図である。
【図３０】ドキュメント保護プログラムをリモートサーバ上に配置した状態を示す図

である。

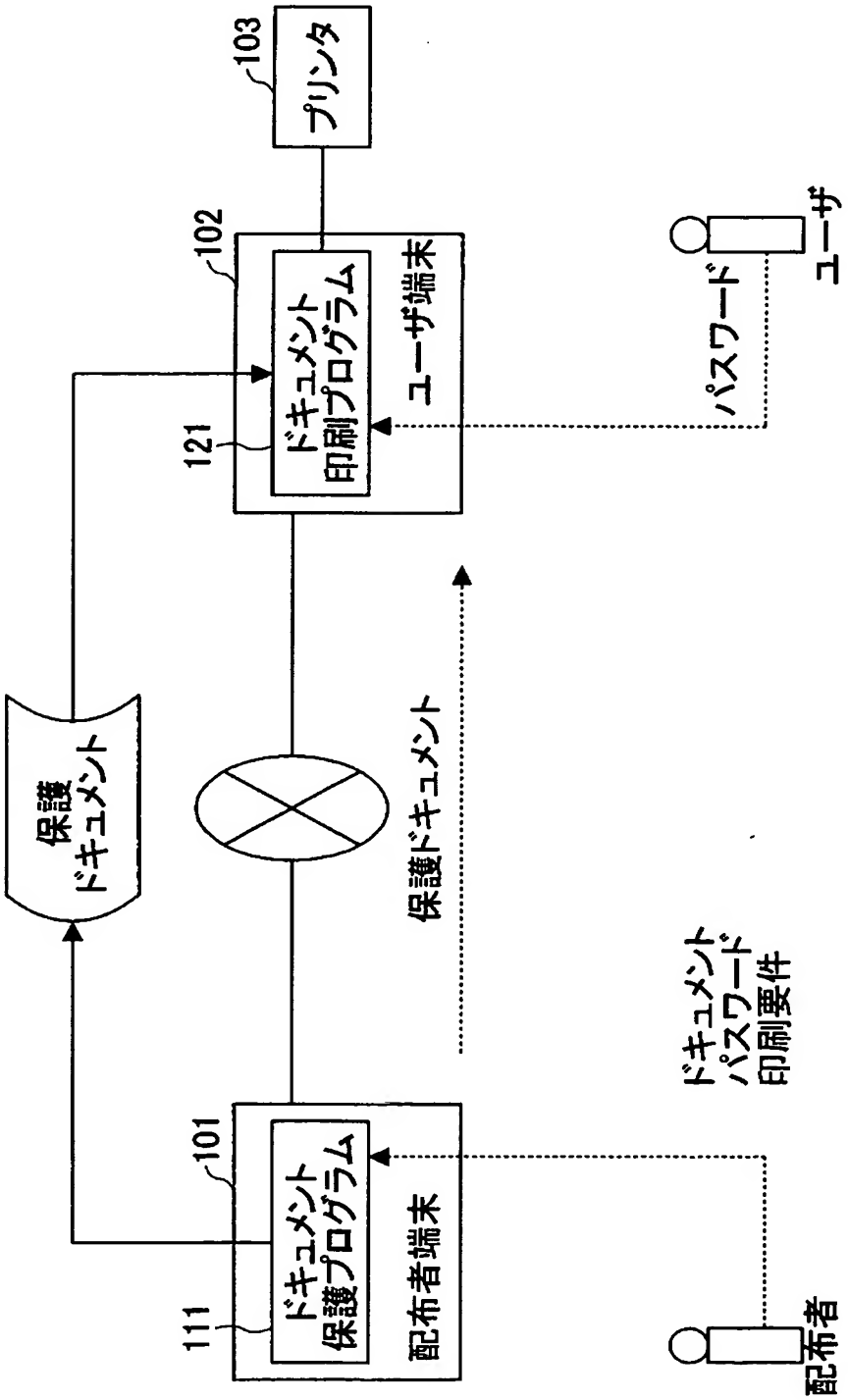
【符号の説明】

【０１７９】

１０１	配布者端末
１０２	ユーザ端末
１０３	プリンタ
１１１	ドキュメント保護プログラム
１２１	ドキュメント印刷プログラム
１１１ａ	属性付与部
１１１ｂ	暗号化部
１１１ｃ	暗号鍵取得部
１１１ｄ	パラメータ取得部
１２１ａ	復号部
１２１ｂ	復号鍵取得部
１２１ｃ	パラメータ取得部
１２１ｄ	印刷要件取得部
１２１ｅ	印刷処理部
１２１ｆ	要件処理部
１２１ｇ	ドキュメント加工部
１２１ｈ	プリンタドライバ
１２１ｉ	警告表示部
１２１ｊ	ログ記録部
２０１	配布者端末
２０２	ユーザ端末
２０３	プリンタ
２０４	アクセスコントロールサーバ
２１１	ドキュメント保護プログラム
２２１	ドキュメント印刷プログラム
２４１	ユーザデータベース
２４２	ＡＣＬデータベース
２１１ａ	暗号化部
２１１ｂ	暗号鍵取得部
２１１ｃ	属性付与部
２１１ｄ	属性登録部
２１１ｅ	パラメータ取得部
２２１ａ	復号部
２２１ｂ	復号鍵取得部
２２１ｃ	印刷要件取得部
２２１ｄ	印刷処理部
２２１ｅ	要件処理部
２２１ｆ	ドキュメント加工部
２２１ｇ	プリンタドライバ
２２１ｈ	警告表示部
２２１ｉ	ログ記録部
２２１ｊ	パラメータ取得部
２０４ａ	属性ＤＢ登録部
２０４ｂ	ユーザ認証部
２０４ｃ	アクセス権限確認部
２０４ｄ	印刷要件取得送付部

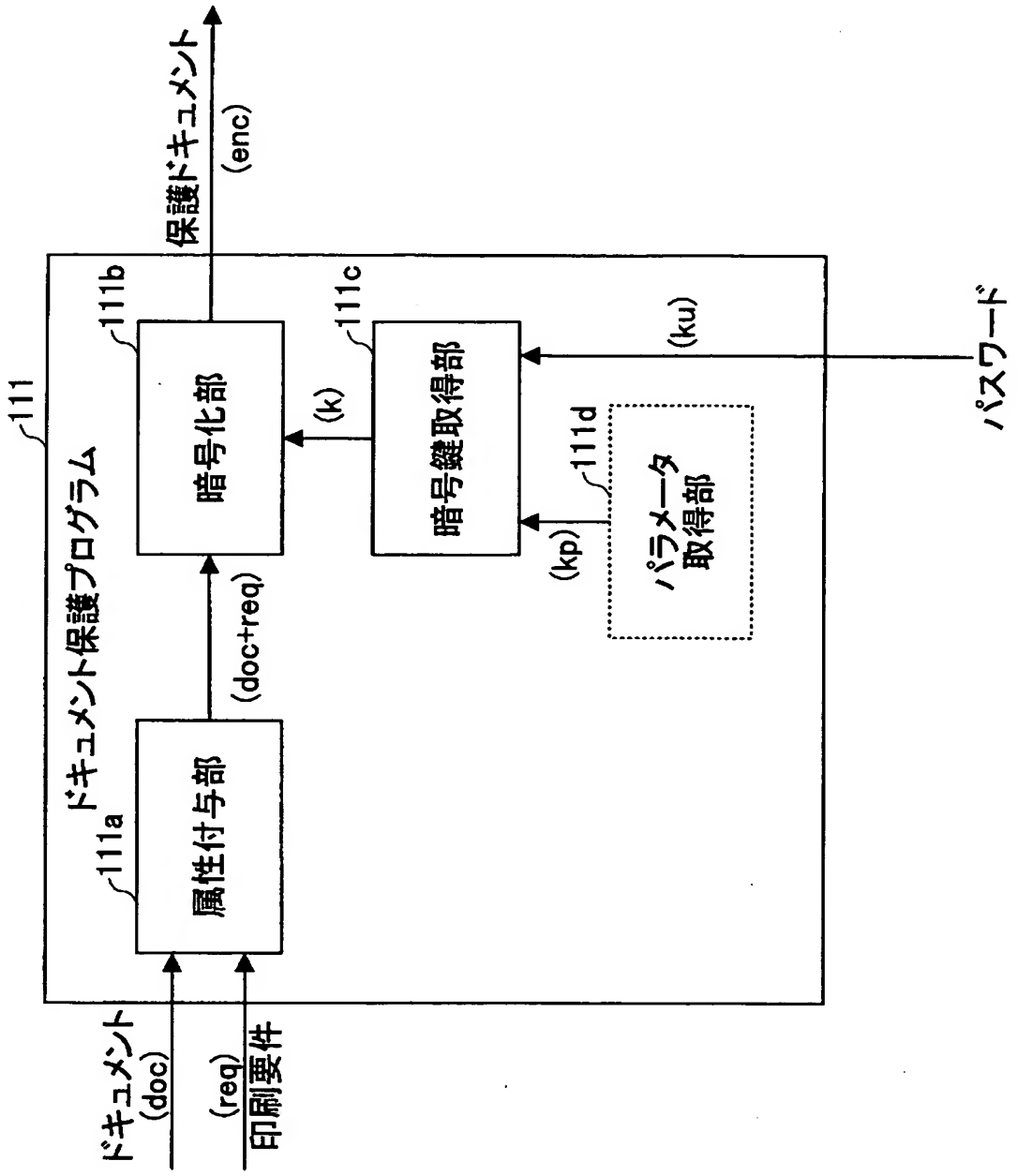
【書類名】図面
【図１】

本発明を好適に実施した第1の実施形態にかかる
ドキュメント保護・印刷システムの構成を示す図



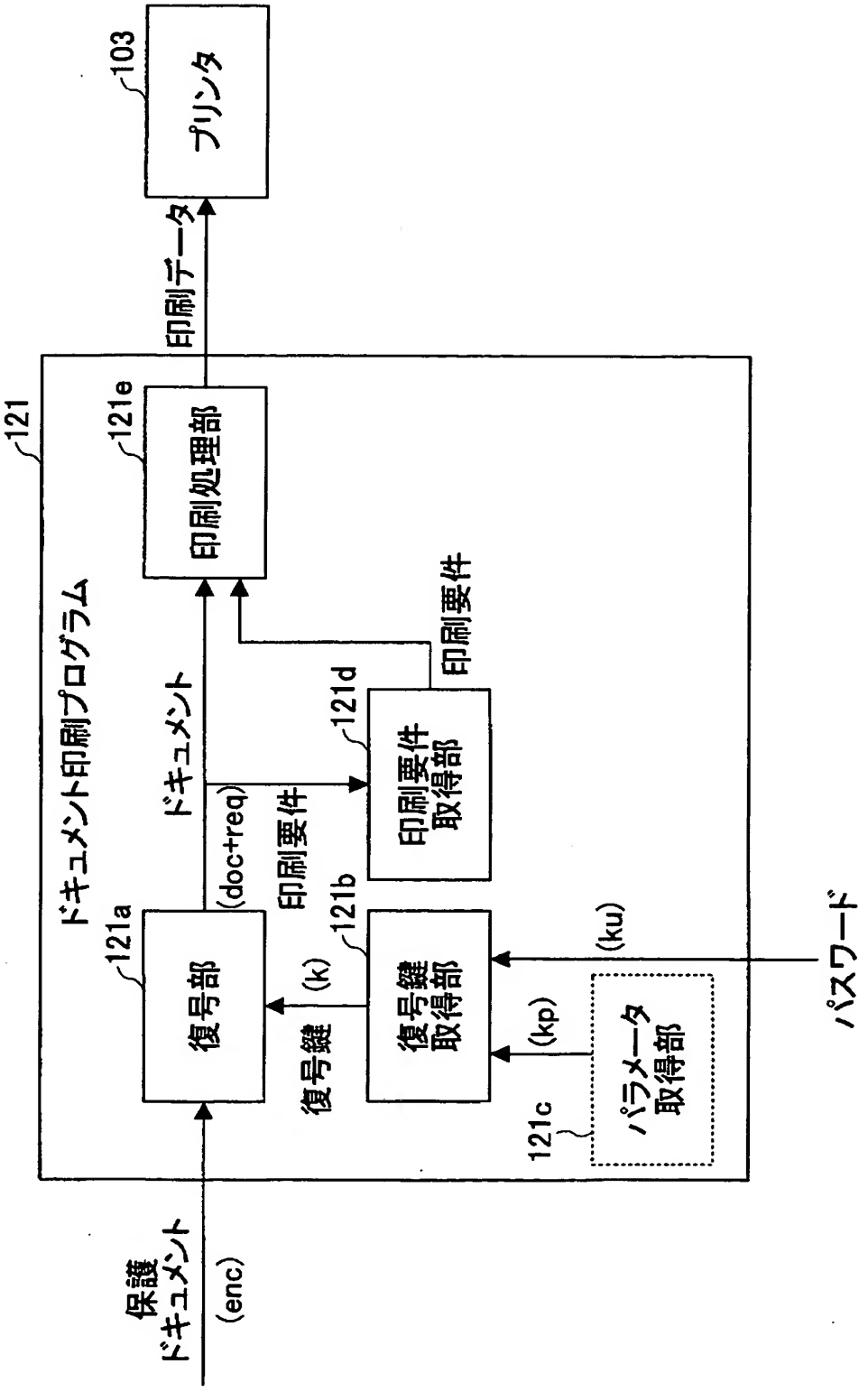
【図２】

ドキュメント保護プログラムの構成例を示す図



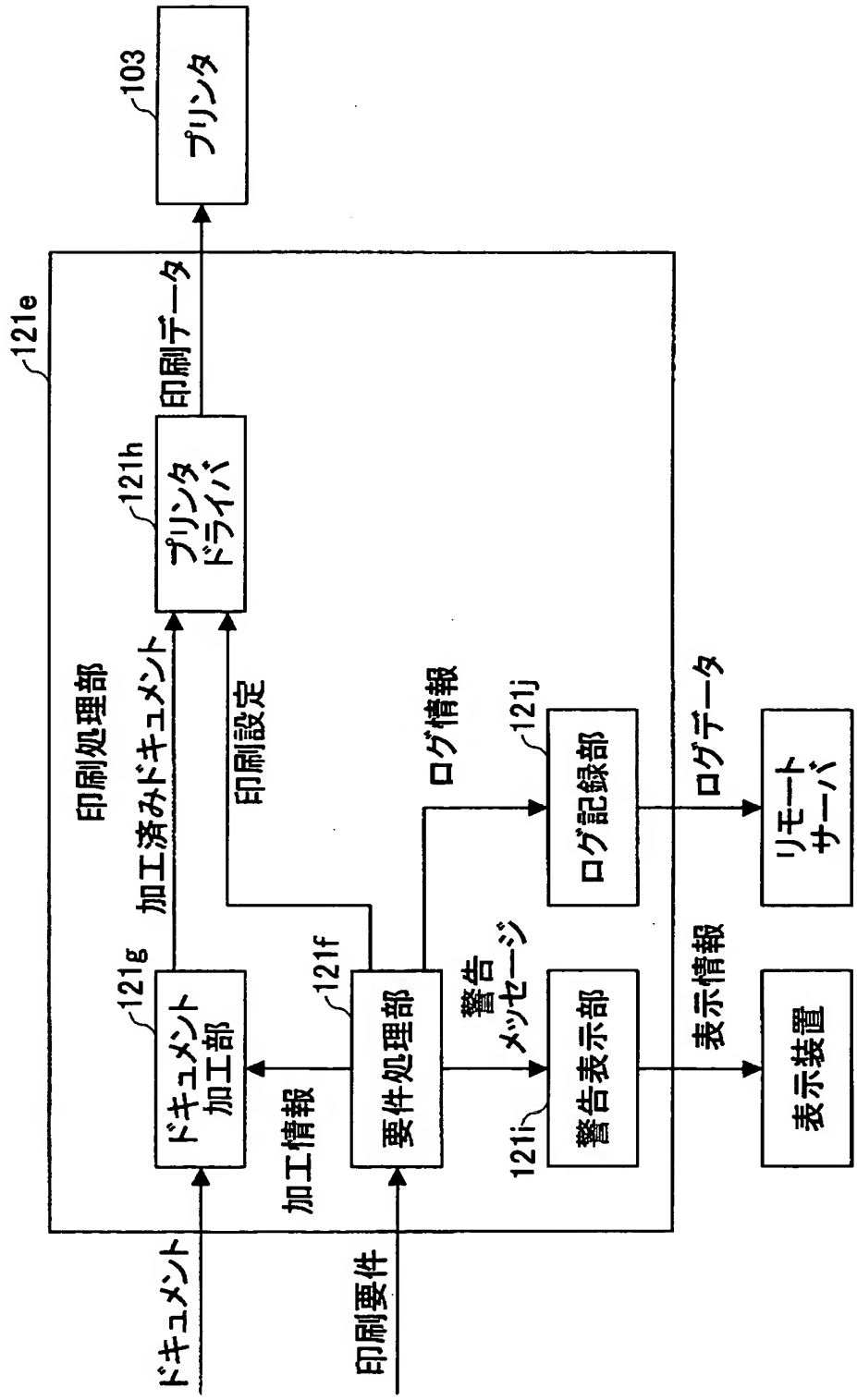
【図３】

ドキュメント印刷プログラムの構成例を示す図



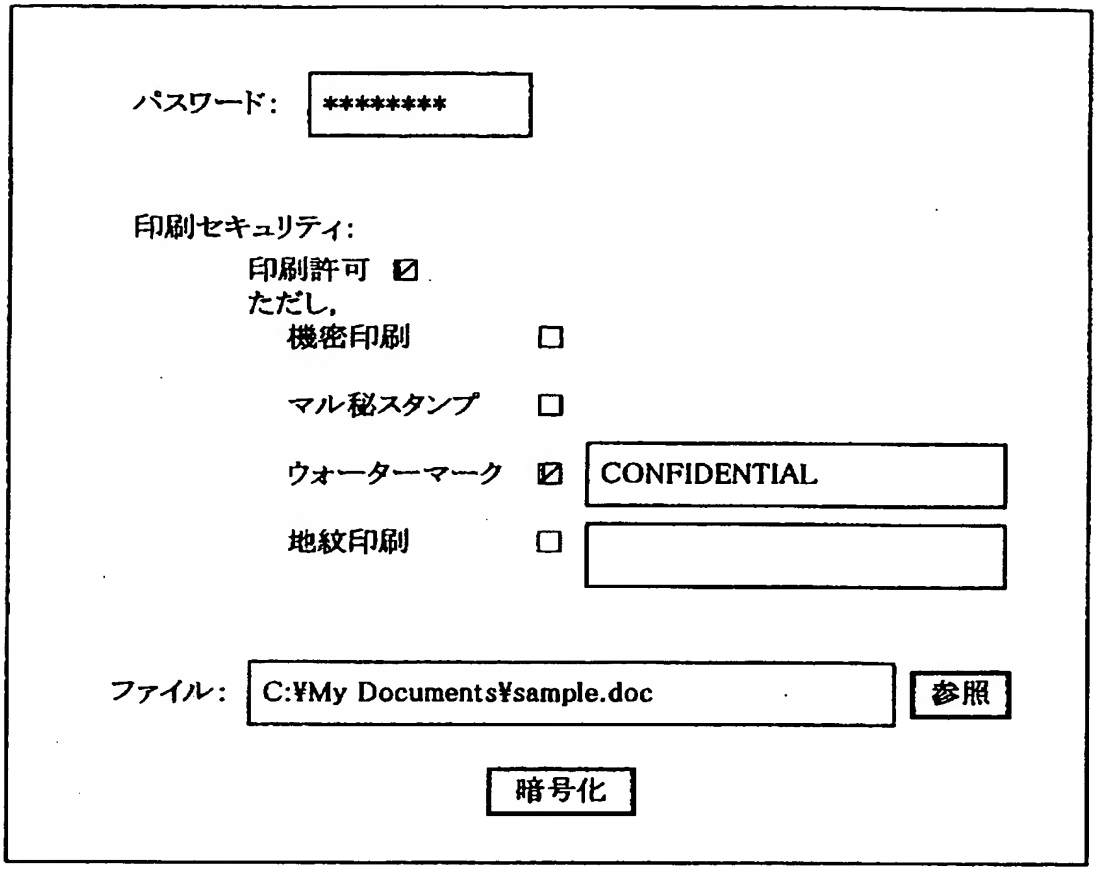
【図４】

印刷処理部の構成例を示す図



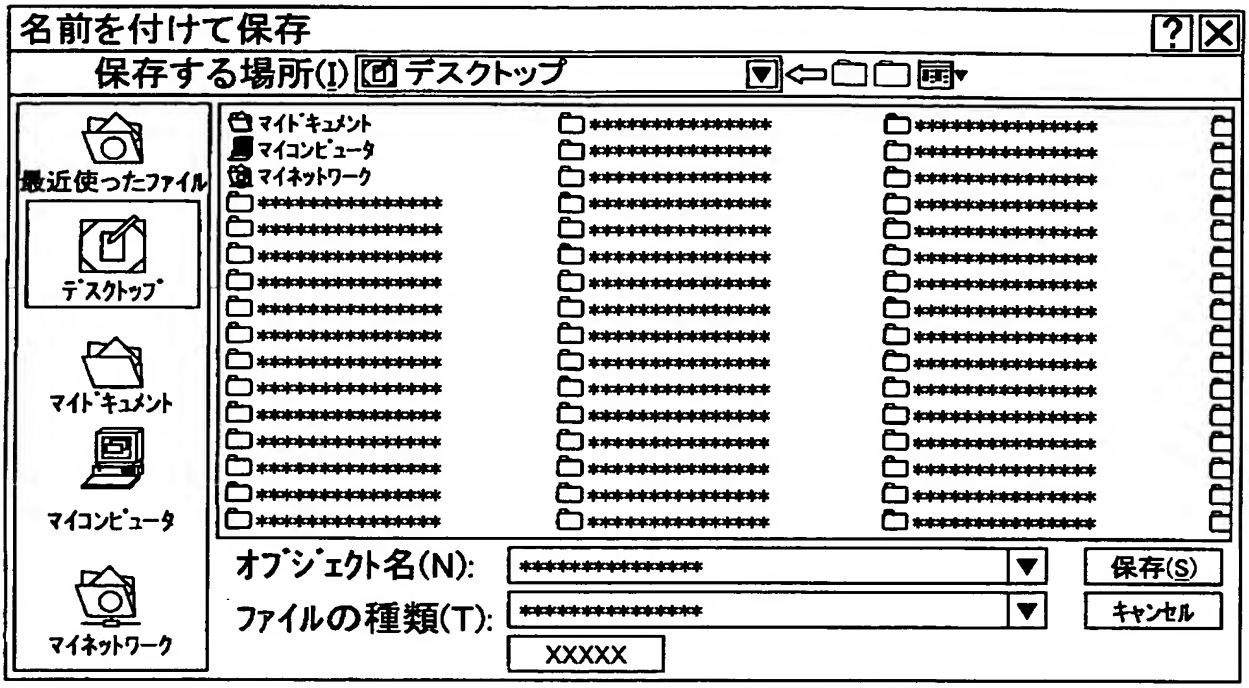
【図５】

パスワードと印刷要件の設定を要求する画面の例を示す図



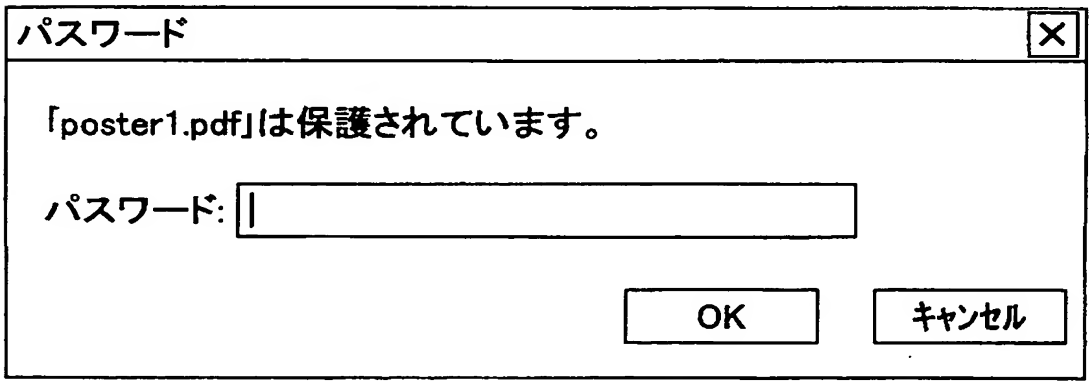
【図６】

保護ドキュメントの保存場所を問い合わせる画面の例を示す図



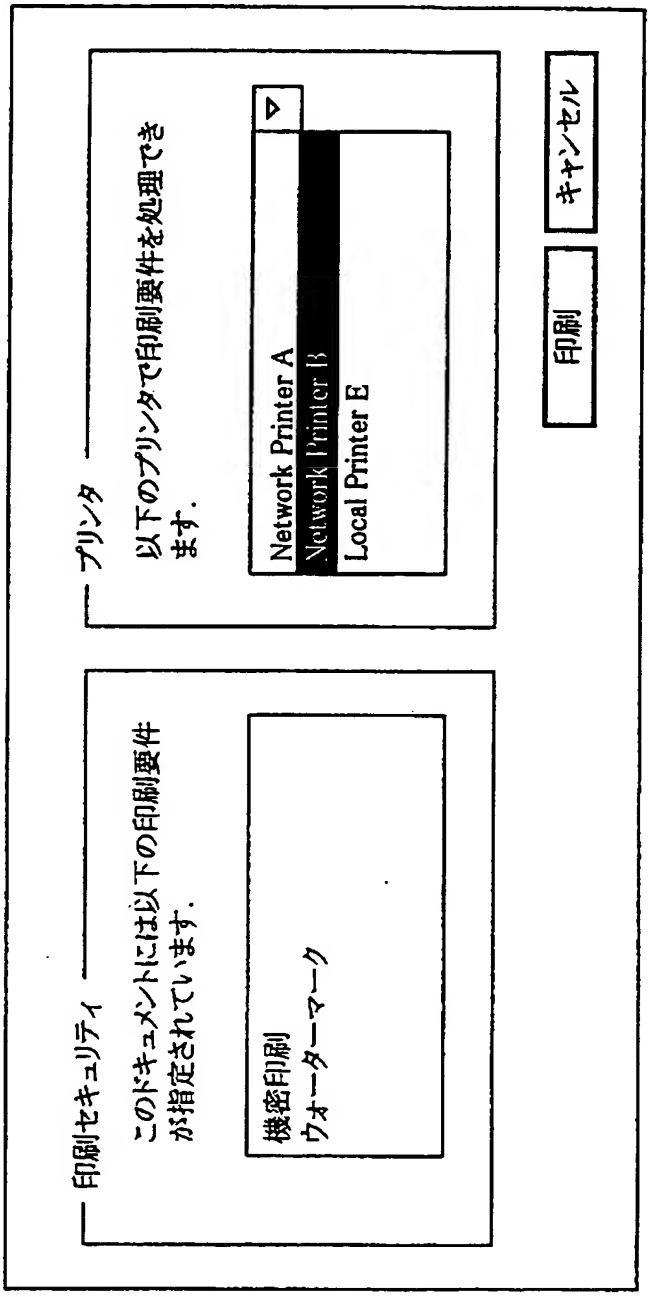
【図７】

パスワードを要求する画面の例を示す図



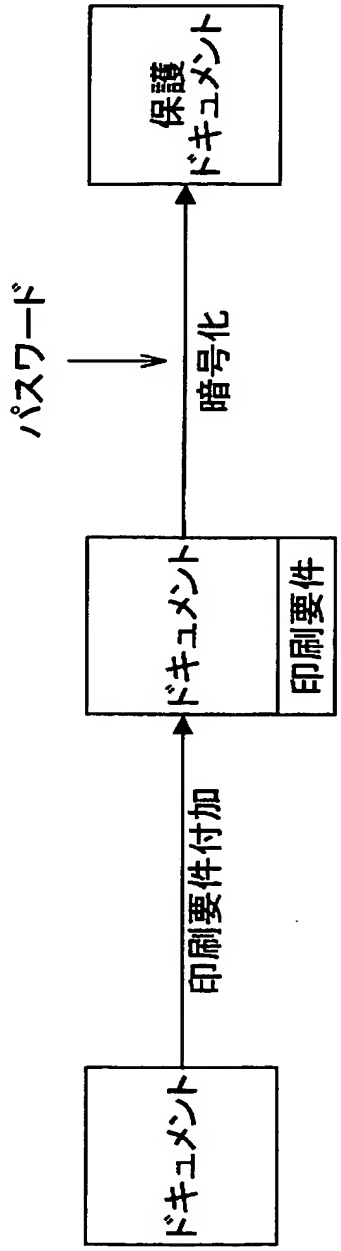
【図８】

ユーザ端末の表示装置上に表示される確認画面の例を示す図



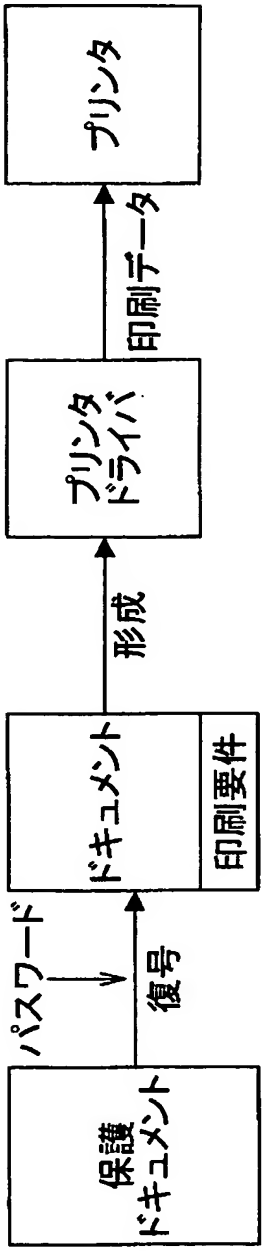
【図９】

第１の実施形態にかかるドキュメント保護プログラムの動作を示す図



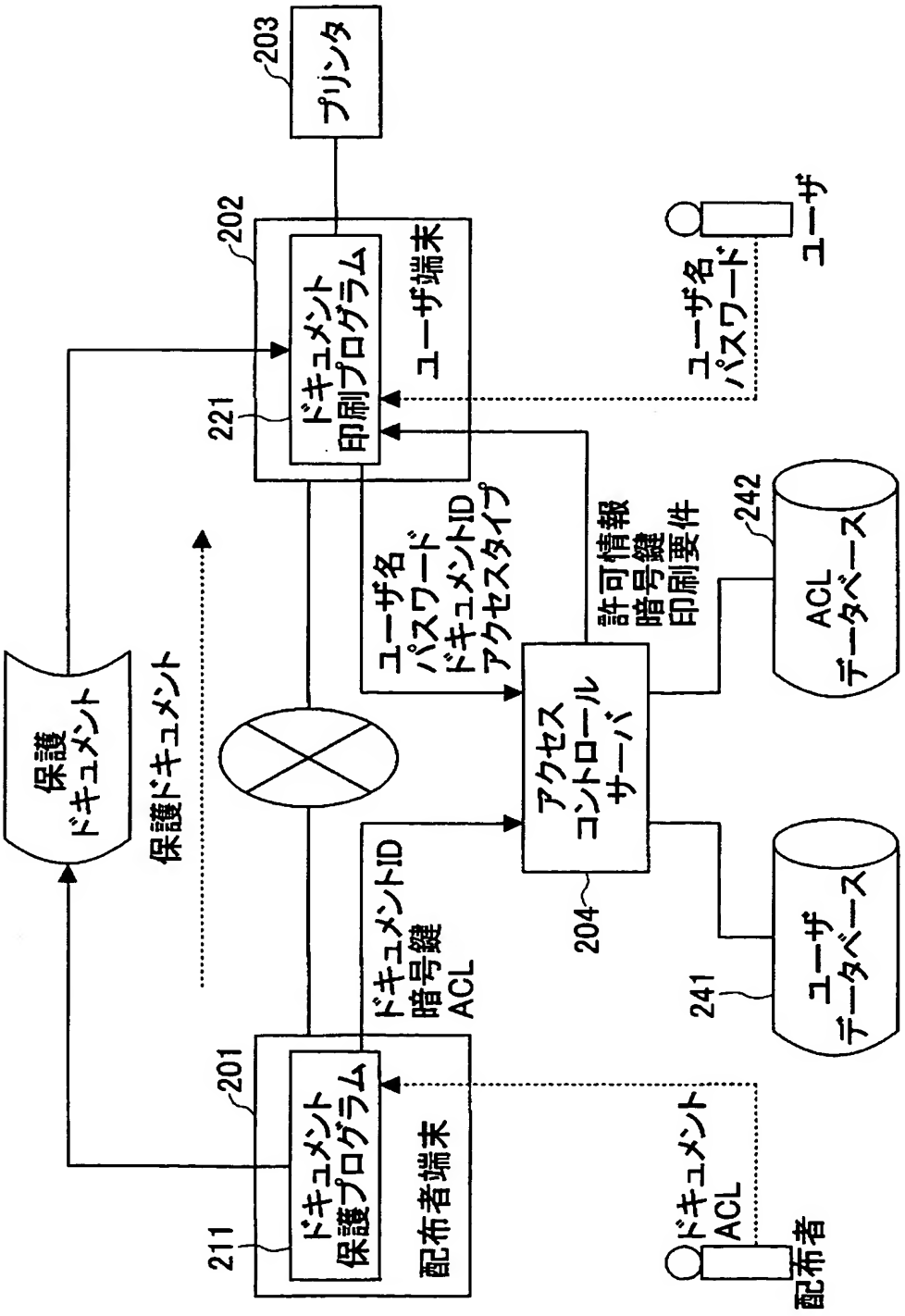
【図１０】

第1の実施形態にかかるドキュメント印刷プログラムの動作を示す図



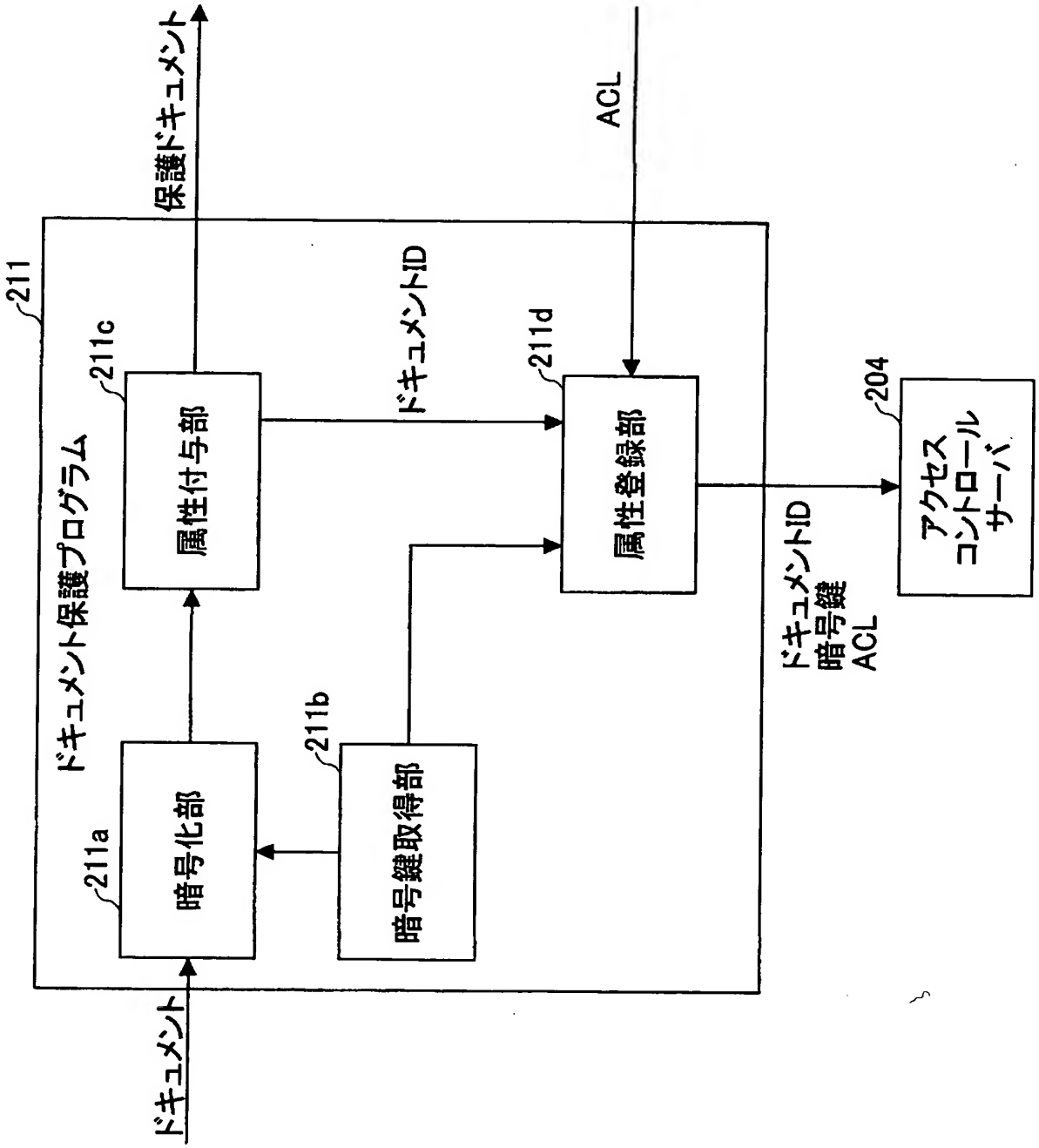
【図１１】

本発明を好適に実施した第2の実施形態にかかるドキュメント保護・印刷システムの構成を示す図



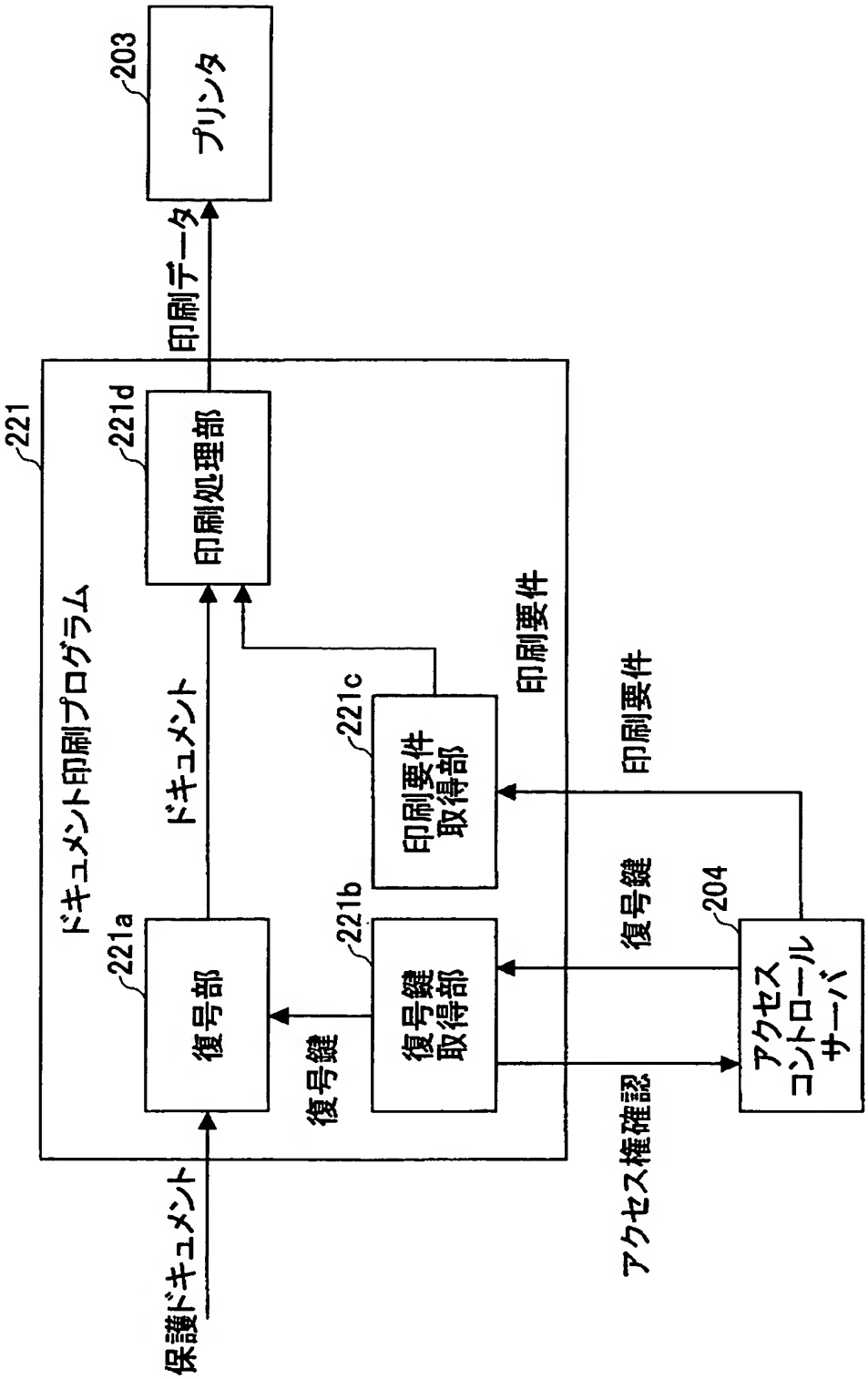
【図１２】

ドキュメント保護プログラムの構成例を示す図



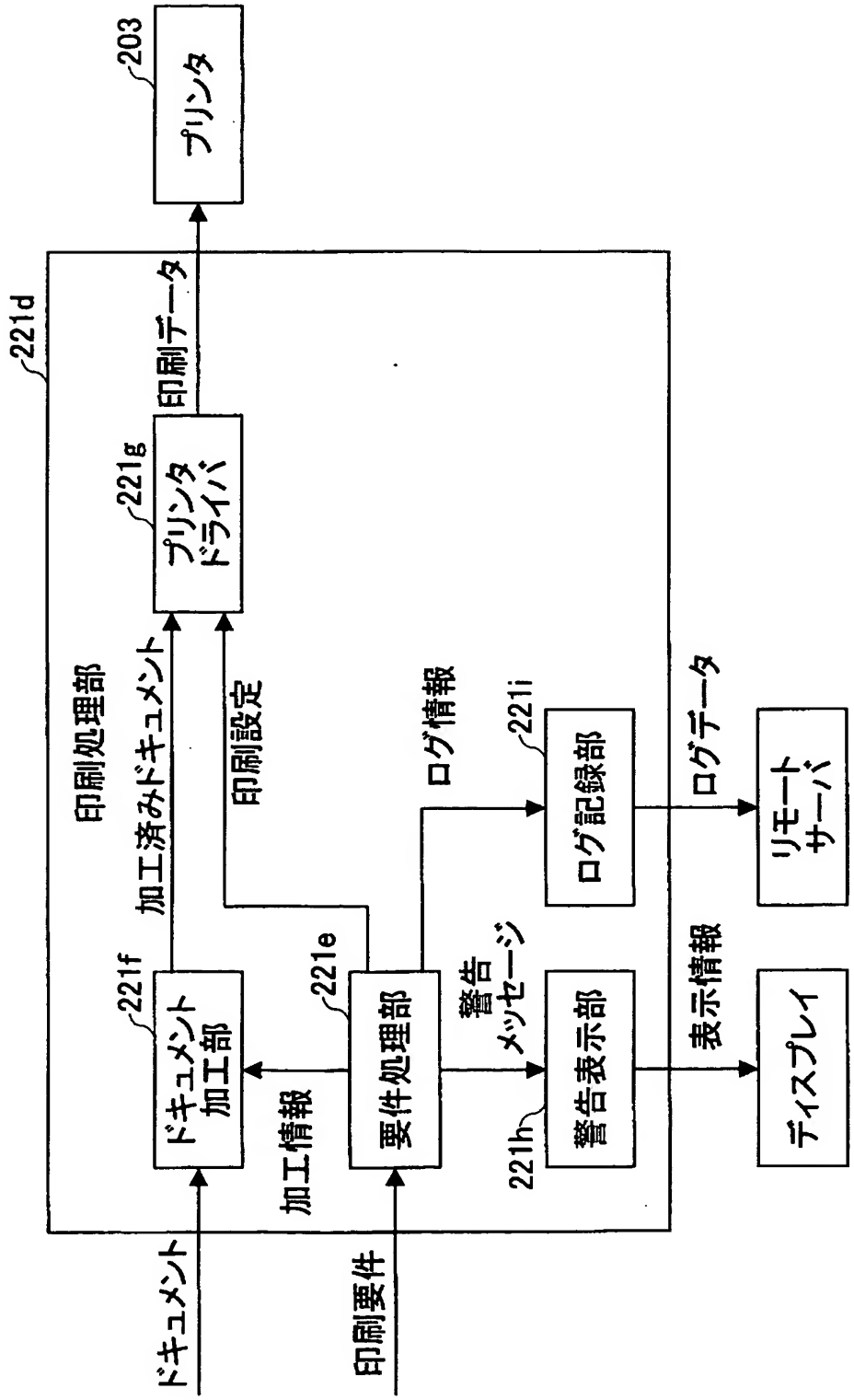
【図１３】

ドキュメント印刷プログラムの構成例を示す図



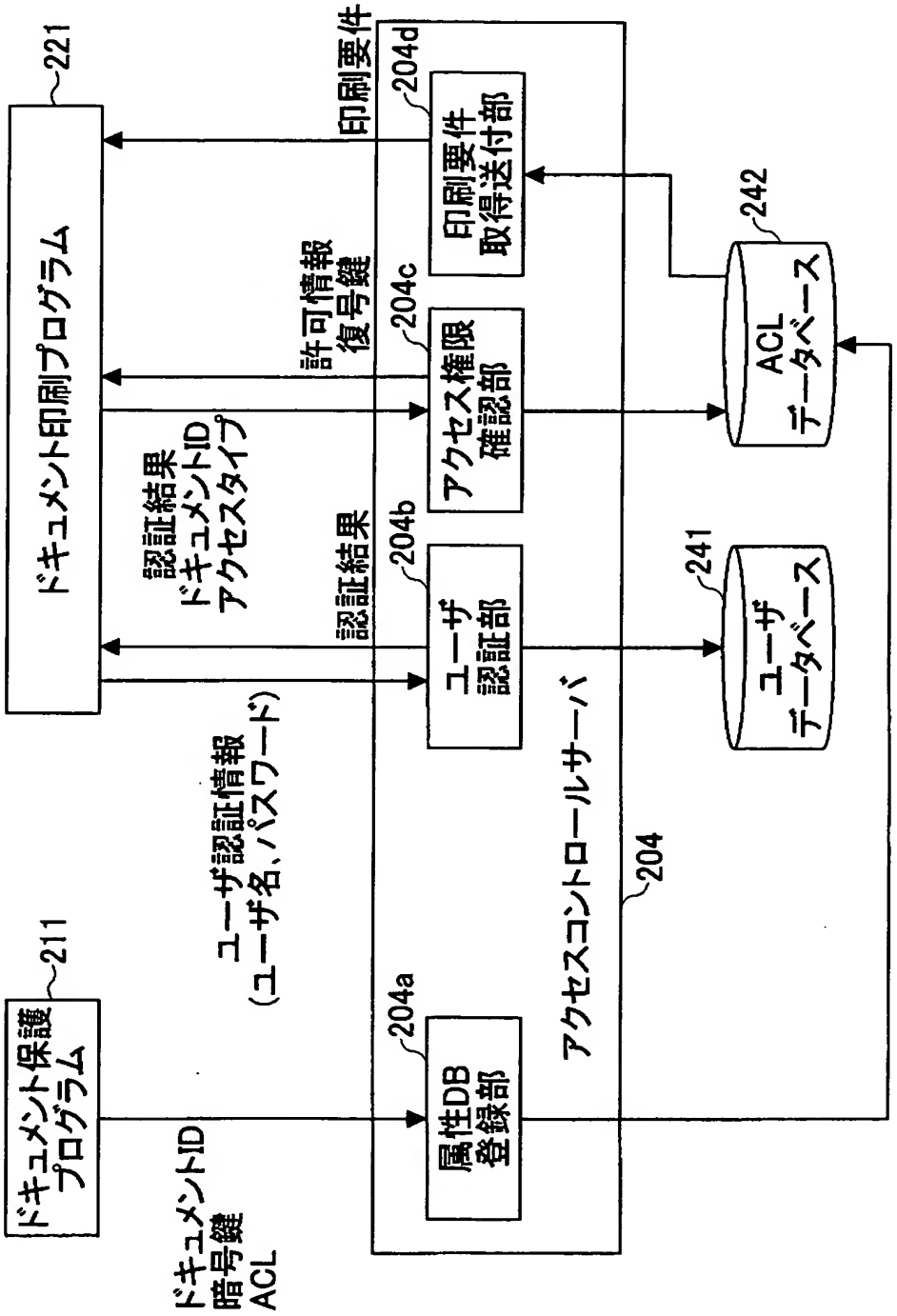
【図１４】

印刷処理部の構成例を示す図



【図１５】

アクセスコントロールサーバの構成例を示す図



【図１６】

ACLの構成例を示す図

User name	Access type	Permission	Requirement
Ichiro	Read	Allowed	—
	Write	Denied	—
	Print	Allowed	PAC(Private Access)
			BDP(Background Dot Patten)
			EBC(Embedding BarCode)
	Hardcopy	Allowed	RAD(Record Audit Date)
Taro	Read	Allowed	—
	Write	Denied	—
	Print	Denied	—
	Hardcopy	Denied	—
⋮			

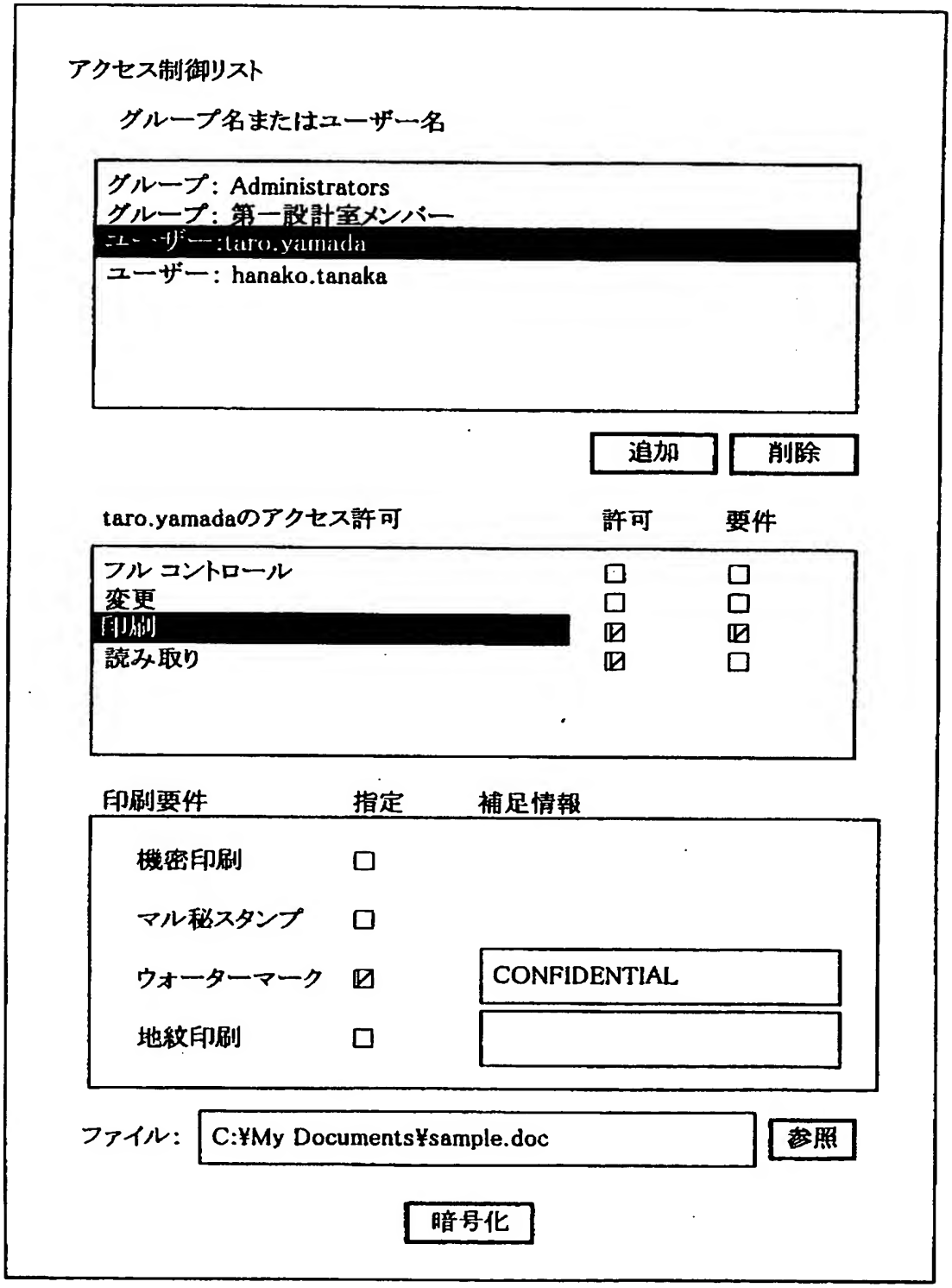
【図１７】

ACLデータベースに記録される情報の構造例を示す図

Document ID	Key	ACL
133.139.234.23.22.125.98.192	89FECA8D2B	(binary data)
133.139.234.23.22.125.99.105	A73C44DA59	(binary data)

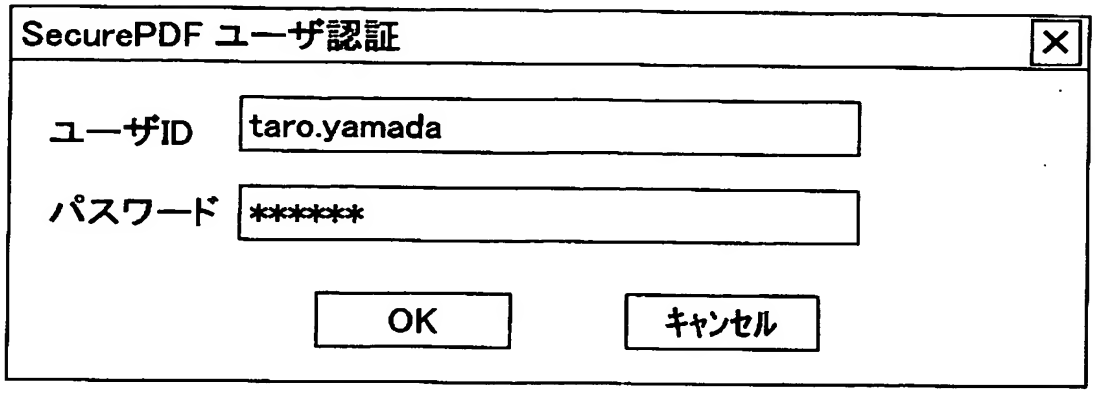
【図１８】

ACLの設定を要求する画面の例を示す図



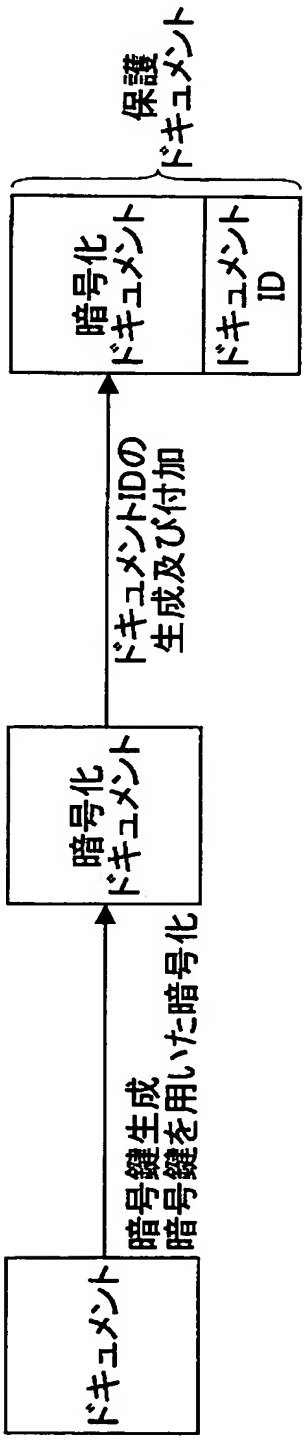
【図１９】

ユーザ名（ユーザID）とパスワードを要求する画面の例を示す図



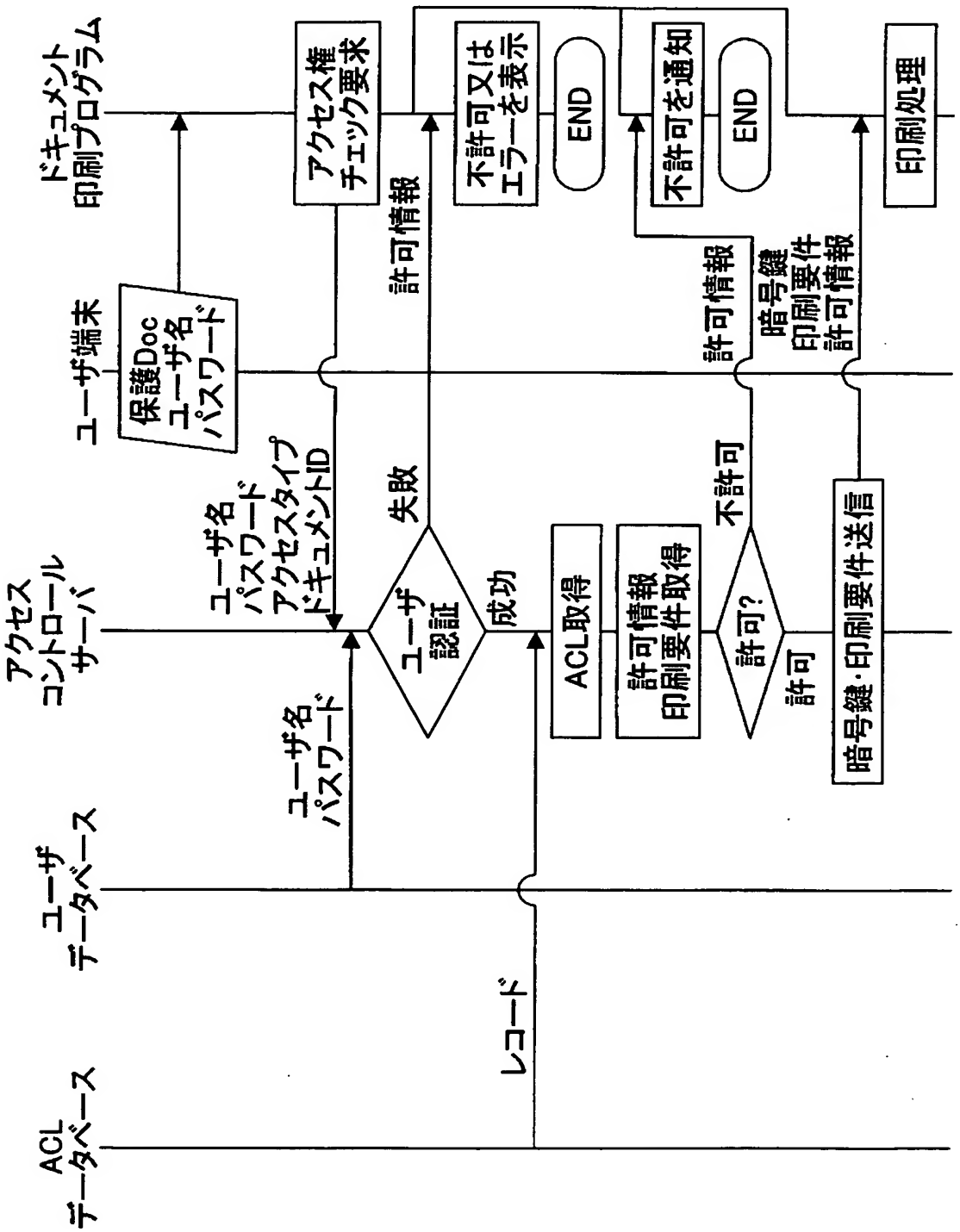
【図２０】

第2の実施形態にかかるドキュメント保護プログラムの動作を示す図



【図２１】

第2の実施形態にかかるドキュメント印刷プログラムおよびアクセスコントロールサーバの動作の流れを示す図



【図２２】

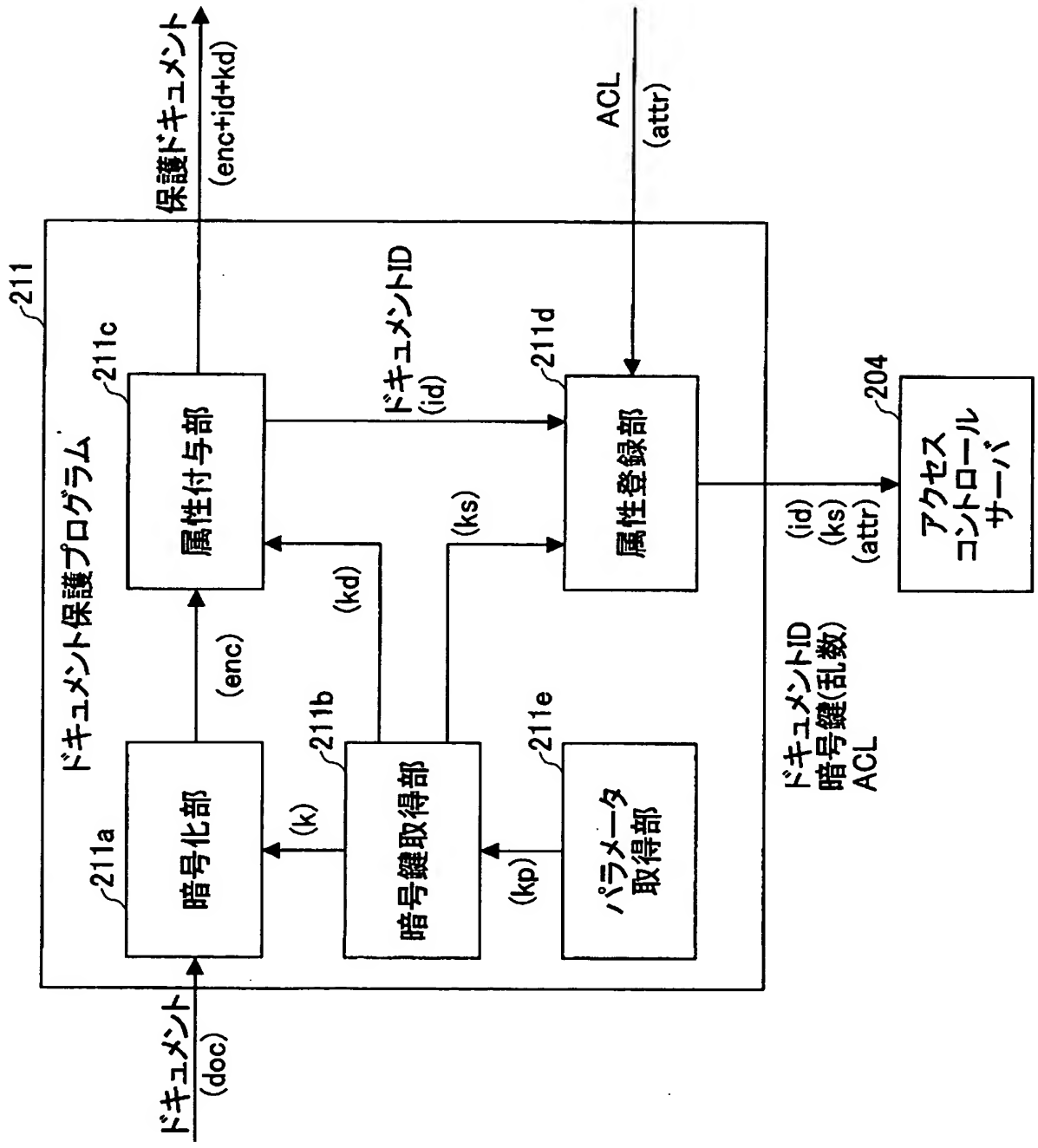
アクセスコントロールサーバへのSOAPによる問い合わせの例を示す図

```
<?xml version="1.0" encoding="UTF-8" ?>
<s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/"
 s:encodingStyle="http://shemas.xmlsoap.org/soap/encoding/">
<s:Body>
<m:isAllowed xmlns:m="http://sample.com/sample">
<sessionId>adfkla;iowoemads</sessionId>
<userId>taro.yamada</userId>
<docId>shm000000000003</docId>
<accessType>print</accessType>
</m:isAllowed>
</s:Body>
</s:Envelope>


<?xml version="1.0" encoding="UTF-8" ?>
<s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/"
s:encodingStyle="http://shemas.xmlsoap.org/soap/encoding/">
<s:Body>
<m:isAllowedResponse xmlns:ns1="http://sample.com/sample">
<isAllowedReturn>
<allowed xsi:type="xsd:boolean">true</allowed>
<requirements>
<item>
<requirement>private_access</requirement>
</item>
<item>
<requirement>watermark</requirement>
<supplement>CONFIDENTIAL</supplement>
</item>
</requirements>
</isAllowedReturn>
</m:isAllowedResponse>
</s:Body>
</s:Envelope>
```

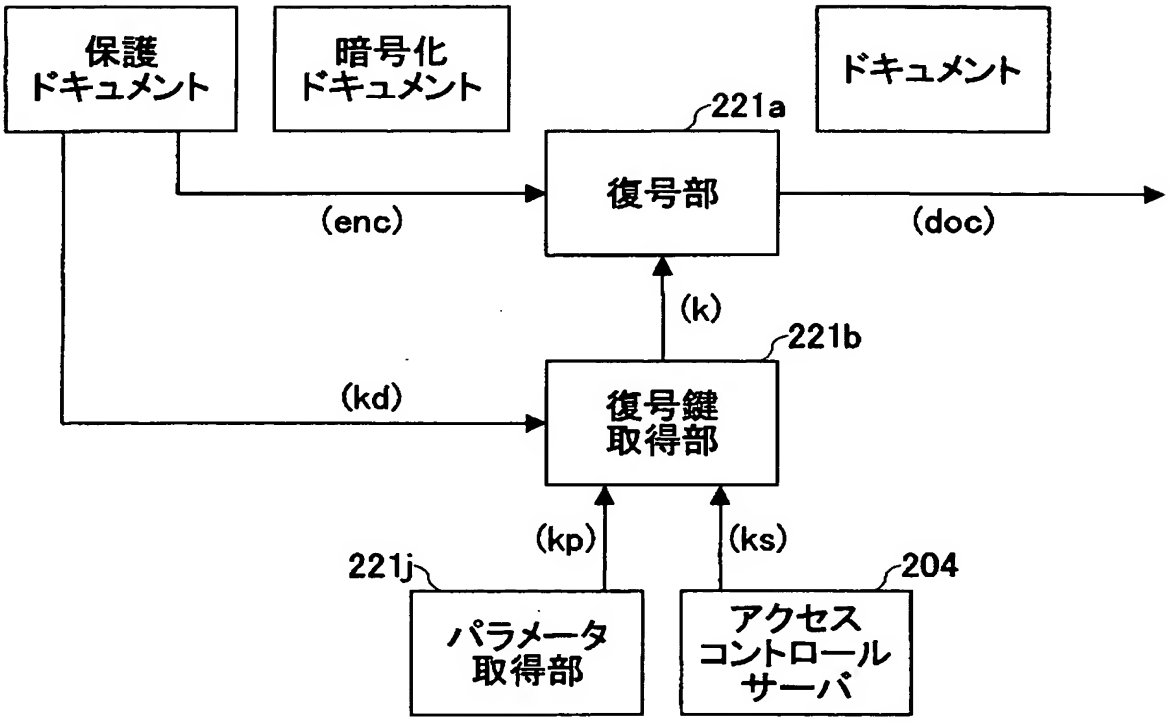
【図２３】

ドキュメント保護プログラムの構成例を示す図



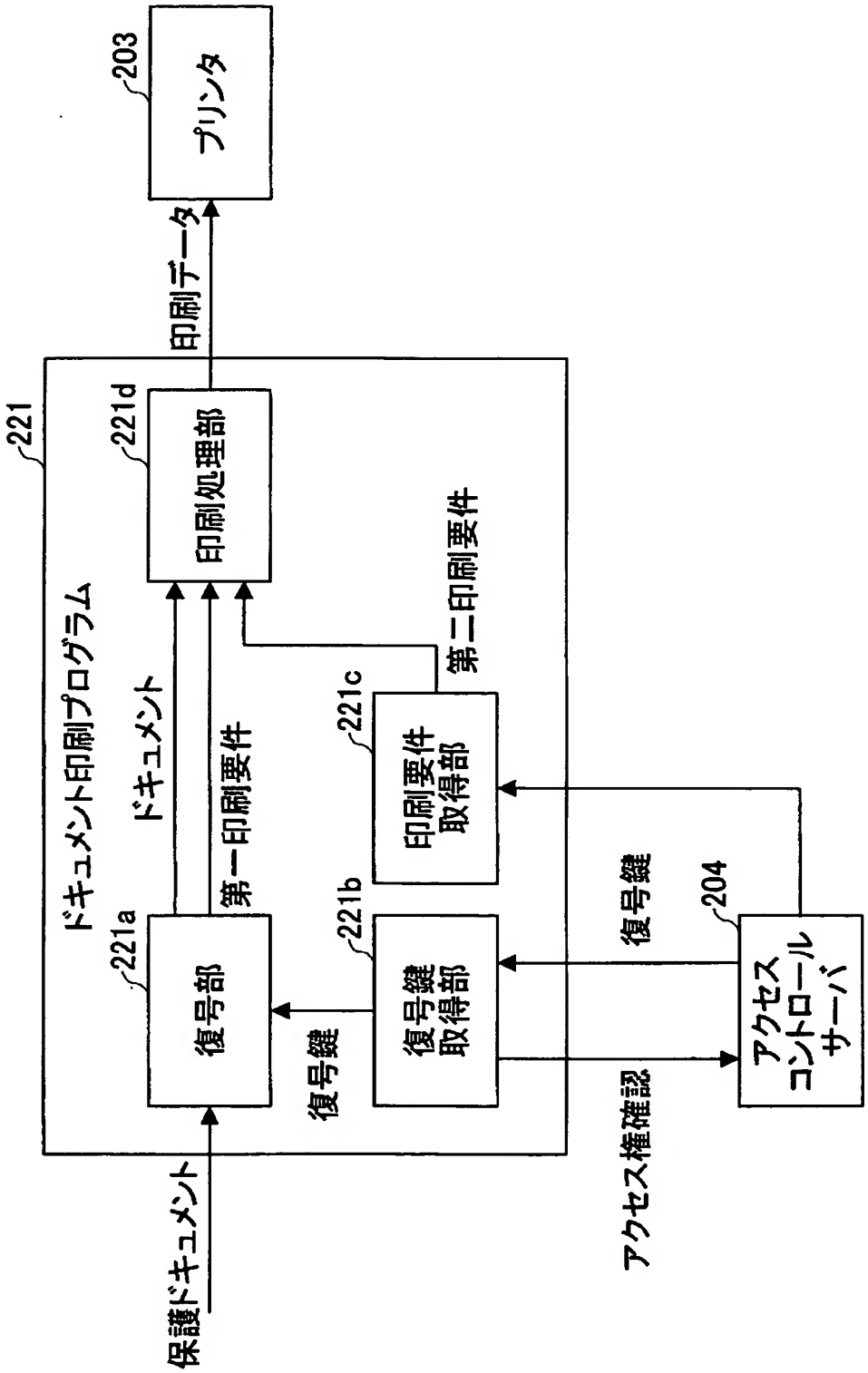
【図２４】

復号の様子を示す図



【図２５】

ドキュメント印刷プログラムの構成例を示す図



【図２６】

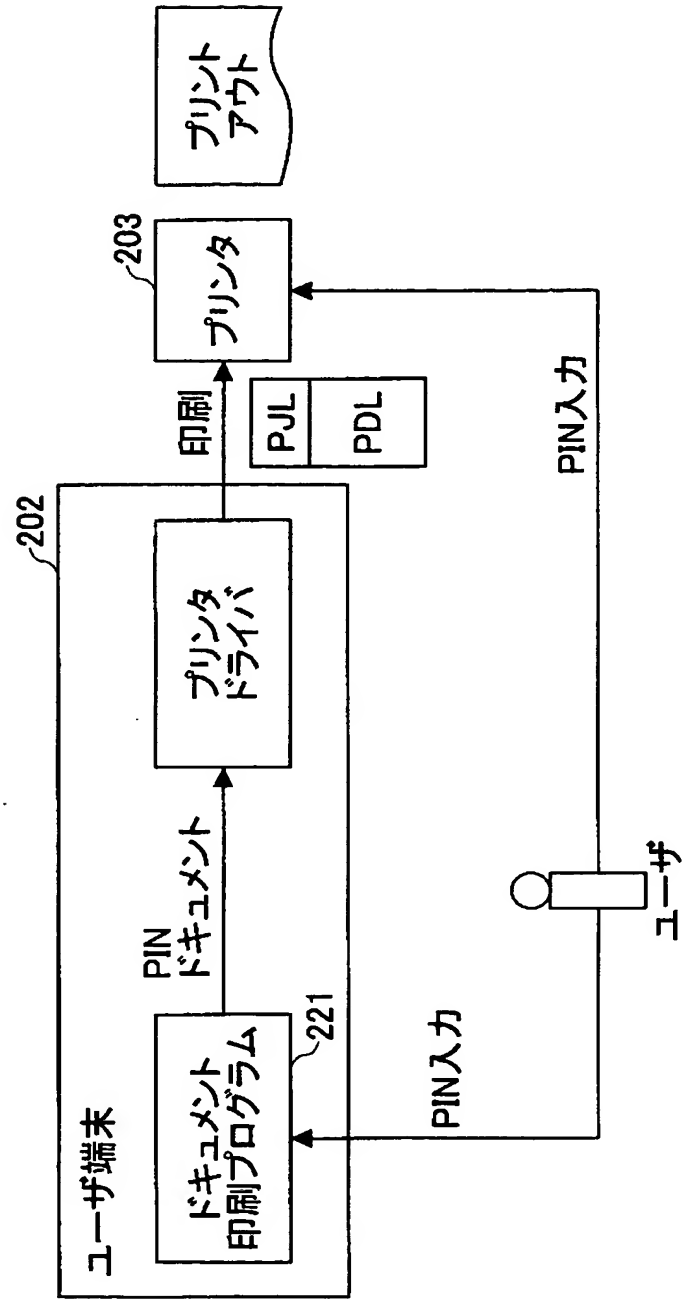
プリンタが備えるセキュリティ機能の例を示す図

プリントセキュリティ機能

スタンプ機能	マル秘などのマークをスタンプやウォーターマークとしてページ内の任意の場所に重ねて印刷する機能。スタンプに使用することができるのは「秘」や「CONFIDENTIAL」などの文字列やビットマップ画像である。
地紋印刷機能	複写機で複写されると特定のイメージが浮き上がるようにコントロールした地紋画像を原稿に重ね合わせて印刷する機能。上記のスタンプ機能でスタンプとして指定する画像を地紋画像にすることで実現する手法が一般的である。
機密印刷機能	印刷を指示する際にプリンタドライバにＰＩＮ（Personal Identification Number）を指定すると、印刷した本人がプリンタのところへ行き、プリンタのオペレーションパネルでそのＰＩＮを入力しなければプリントアウトされない機能。

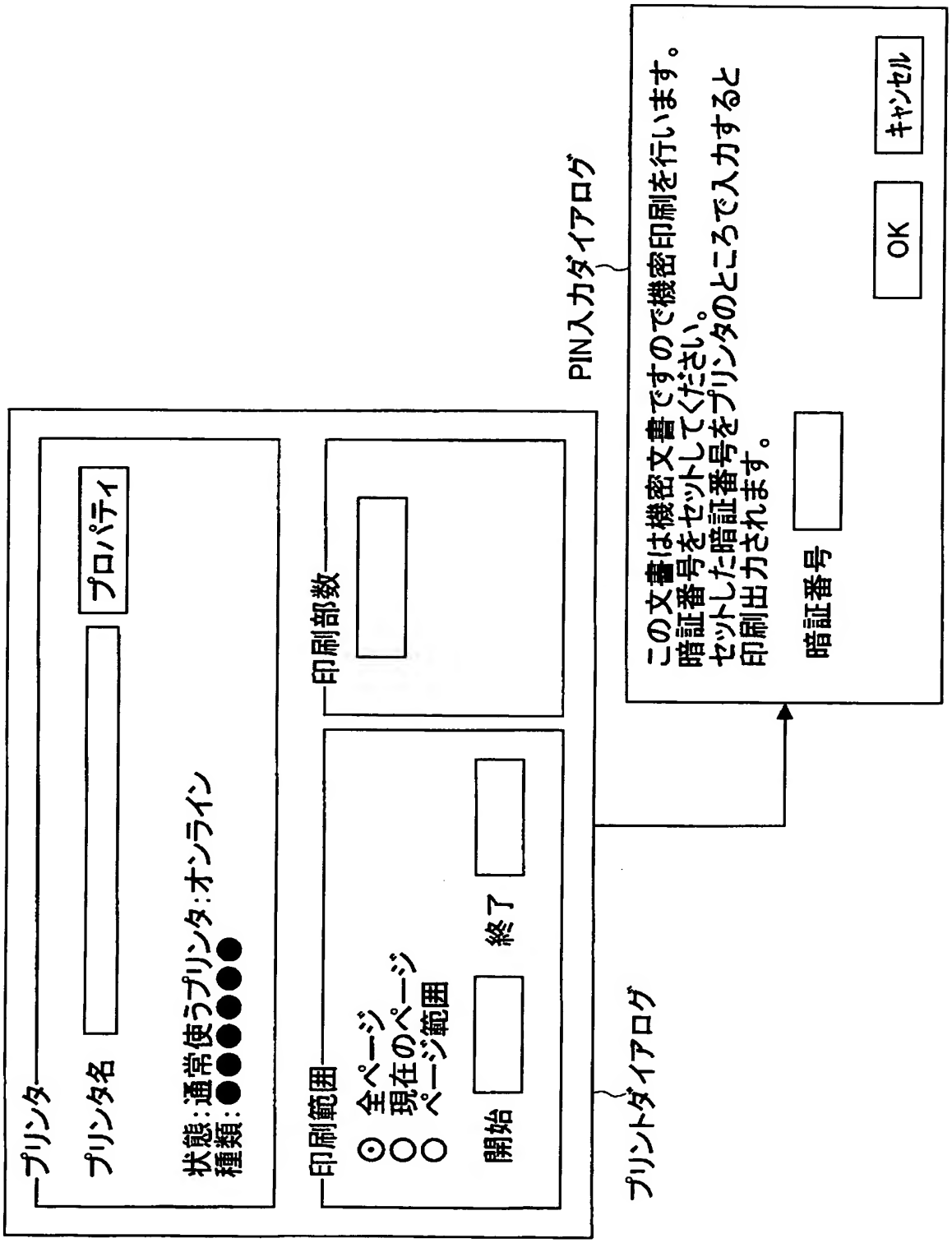
【図２７】

PACが設定されたドキュメントを印刷する際の処理を示す図



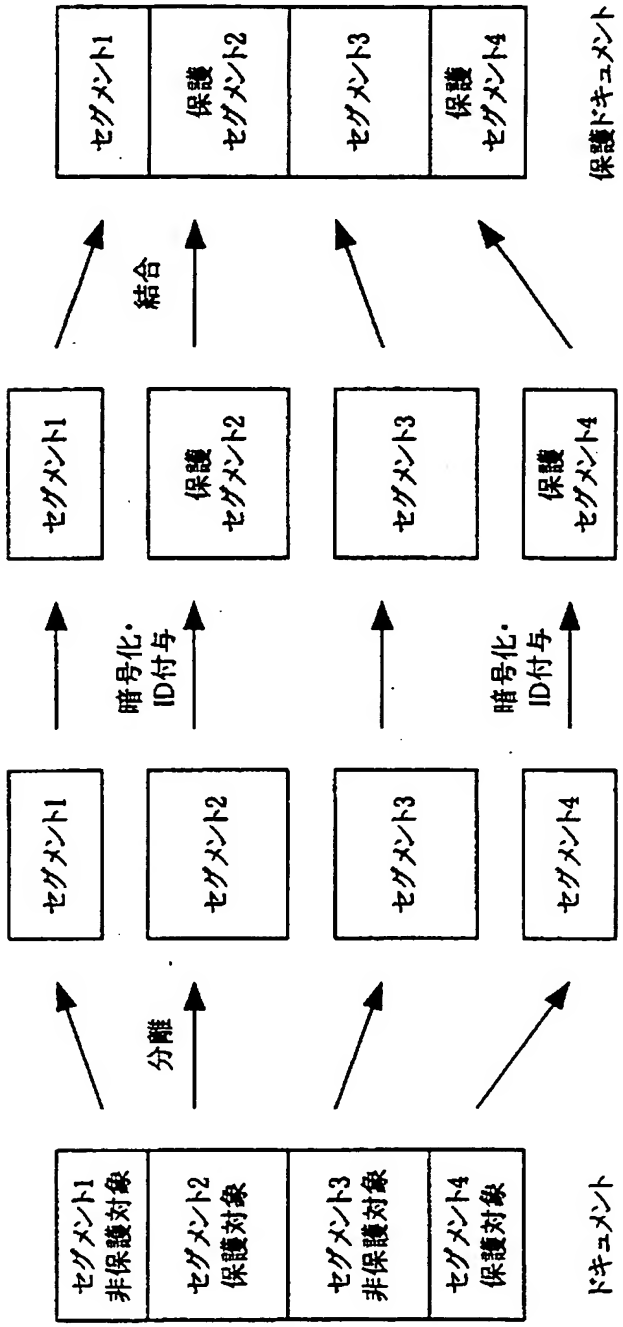
【図２８】

PIN入力のダイアログを示す図



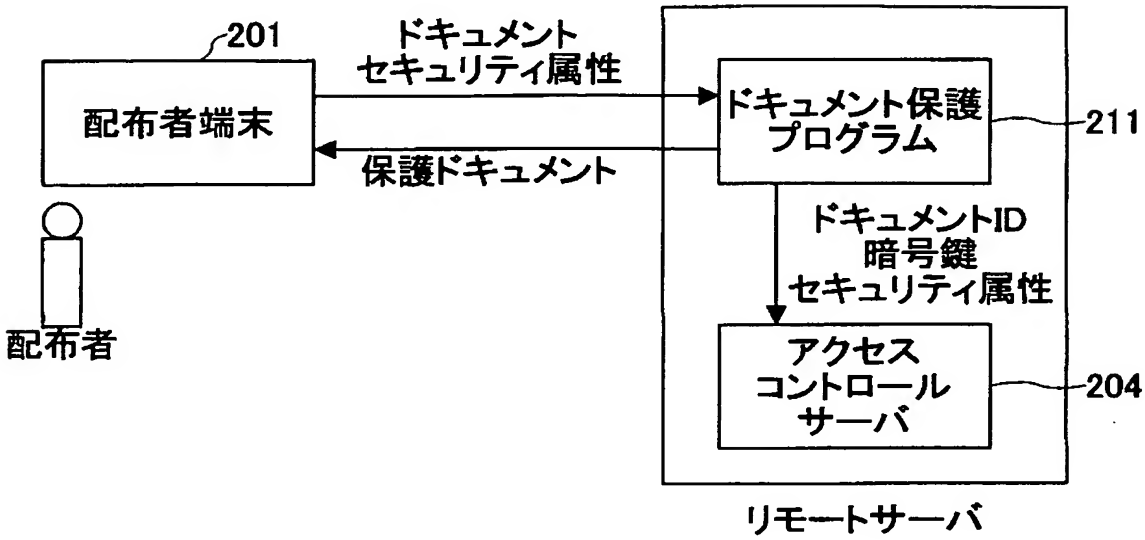
【図２９】

ドキュメントを複数のセグメントに分けて保護する場合の処理を示す図



【図３０】

ドキュメント保護プログラムをリモートサーバ上に配置した状態を示す図



【書類名】要約書
【要約】
【課題】　プリントアウトによるドキュメントの漏洩を防止したドキュメント印刷プログラム、ドキュメント保護プログラムおよびドキュメント保護システムを提供することを目的とする。
【解決手段】　ドキュメントファイルに関連付けられている印刷要件を取得する手段と、上記ドキュメントファイルを印刷する時に上記印刷要件を強制的に実行させる手段とを備えるドキュメント印刷プログラムと、ドキュメントファイルの保護を行うドキュメント保護プログラムとにより構成される。
【選択図】　図１

特願２００３－３１４４６７

出　願　人　履　歴　情　報

識別番号　　［０００００６７４７］

１．変更年月日　　２００２年　５月１７日
［変更理由］　　住所変更
住　所　　東京都大田区中馬込１丁目３番６号
氏　名　　株式会社リコー